

**SUBMISSION No. 113**

**SUBMISSION TO THE JOINT SELECT  
COMMITTEE ON CYBER-SAFETY FROM  
THE CONSULTATIVE WORKING GROUP ON  
CYBERSAFETY**

**14 JULY 2010**

## Contents

<b>Section</b>	<b>Heading</b>	<b>Page</b>
1	Executive Summary	1
2	Background	10
3	Approach taken by the Consultative Working Group (CWG)	10
4	Findings to date and next steps	11
4.1	The online environment in which Australian children currently engage	11
4.2	The nature, prevalence and implications of cybersafety threats	13
4.3	Australian and international responses to current cybersafety threats	15
4.4	Opportunities for cooperation across Australian stakeholders and with international stakeholders	29
4.5	Information required to realise the potential for achieving and continuing world's best practice safeguards	31
4.6	Ensuring that the CWG's deliberations take account of new technologies	35
4.7	Review mechanisms	38
5	Operation of the CWG	39
6	References	39
7	Attachments	
7.1	Attachment A: CWG Membership 2010-2011	
7.2	Attachment B: CWG Terms of Reference	
7.3	Attachment C: Examples of Australian cybersafety and youth outreach initiatives, and unpublished Australian research	
7.4	Attachment D: Agreements on common rules and principles for the protection of young people using social networking sites	
7.5	Attachment E: Examples of Australian cybersafety and youth outreach initiatives	
7.6	Attachment F: YouTube safety and integrity elements	

## 1. Executive Summary:

The Australian Government's Consultative Working Group on Cybersafety (CWG) is an initiative of the Government's Cybersafety Plan. The CWG is comprised of representatives from industry, community organisations and Australian Government agencies. The CWG's role is to consider all aspects of cybersafety faced by Australian children, provide information to Government on measures required to operate and maintain world's best practice safeguards for Australian children engaging in the digital economy and advise the Government on priorities for action by government and industry.

This submission outlines the findings and outputs of the CWG over the period of its operation from May 2008 to June 2010 and reflects the content of its first report to the Minister for Broadband, Communications and the Digital Economy, Senator the Hon Stephen Conroy.

The CWG's terms of reference specify six areas of focus for the Group. These are:

1. the online environment in which Australian children currently engage
2. the nature, prevalence and implications of cybersafety risks
3. Australian and international responses to current cybersafety risks
4. opportunities for cooperation across Australian stakeholders and with international stakeholders
5. information required to realise the potential for achieving and continuing world's best practice safeguards, and
6. ensuring that the CWG's deliberations take account of new technologies.

In undertaking its work the CWG is mindful that young people's engagement with the internet brings more benefits than not, and that their successful engagement with the digital economy will be essential for their own future and that of Australia as a whole. The CWG therefore intends to continue to focus on factors influencing children's engagement in the online environment.

The Australian Communications and Media Authority (ACMA) suggests that applying measures along multiple points of the supply chain for online content and services is the most effective approach (ACMA 2008). The CWG notes that the Government's current cybersafety strategy incorporates a multifaceted approach that is consistent with this understanding.

The CWG considers that measures to combat cybersafety threats fall under a number of key areas. These include:

- research and consultation
- education, awareness and assistance
- regulation and law enforcement
- technical measures, and
- international cooperation.

### *Research and consultation*

The CWG has provided advice on two research projects commissioned by the Department. Both will increase the Government's understanding of cybersafety threats to Australian children and assist in fine tuning policy. The outcome of both will be considered by the CWG as a basis for future advice to Government. The two research projects are:

- a review and analysis of existing Australian and international research on cybersafety undertaken by Edith Cowan University, and
- development and implementation of a repeatable survey designed to collect information from parents, teachers and others on cybersafety and cyber security issues that will enable tracking over time of changes in behaviour.

These projects will augment research undertaken by other Government bodies, such as the ACMA and the Australian Bureau of Statistics (ABS). The Department of Education, Employment and Workplace Relations (DEEWR) has also funded a number of investigative studies including two specifically on covert bullying (which includes cyber-bullying), which have added to the body of knowledge about the extent and impact of cyberbullying. In addition, the Attorney-General's Department has commissioned a review of online grooming which the CWG will be considering as it works through these issues.

The Government's main vehicles for cybersafety consultation are the CWG and the Youth Advisory Group on Cybersafety. The CWG considers that the Youth Advisory Group will continue to be crucial in providing the views of children and young people in terms of:

- the nature of children's online engagement
- emerging cybersafety risks, and
- how best to tackle these risks from a young person's perspective.

The Youth Advisory Group has already provided valuable advice on preferred measures to improve cybersafety, particularly in the area of cyber-bullying.

Research and consultation is also being undertaken in other Australian jurisdictions, as well as by industry and non government organisations. The CWG notes, for example, that the NSW Legislative Council completed its inquiry into Bullying of Children and Young People. The NSW Government tabled its response to the report on 12 May 2010 outlining the actions that Government has planned to address bullying and cyber-bullying and outlined an increased emphasis on greater coordination and cooperation across all levels of government, school systems, schools, the community, and researchers in efforts to address bullying.

Research and consultation will be an ongoing task for the CWG, in order that cybersafety programs and policies retain relevance to the experiences of Australian youth.

### *Education, awareness and assistance*

Across Australia, significant effort has gone into developing cybersafety education, awareness and assistance programs and policies—the CWG has undertaken a limited stock-take of these. In terms of the Australian Government, key bodies undertaking work in this field include the Department of Broadband, Communications and the

Digital Economy (DBCDE), the ACMA, the Australian Federal Police (AFP), DEEWR and the Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA).

- DBCDE has developed the Stay Smart Online website as a key source of information for all Australians on the simple steps they can take to be secure and confident online. This website hosts a free Alert Service that provides information in plain language on the latest cyber security threats and vulnerabilities.
- The ACMA operates, among other measures, an outreach program targeting teachers, children and their parents. This includes the national roll out of internet safety awareness presentations for students, teachers and parents, national rollout of an accredited professional development program for teachers and the recent launch of a pre-service teacher training program. An interactive and innovative e-learning platform is also under development to complement and build on the information and knowledge being delivered by these face to face presentations and workshops.
- In mid 2009 the ACMA launched its Cybersmart website ([www.cybersmart.gov.au](http://www.cybersmart.gov.au)), providing free access to internet safety and advice as well as to an extensive range of teaching resources. The site includes referral mechanisms for the reporting of offensive content, links to the AFP to report suspicious online behaviour, and also the Cybersmart online helpline.
  - The Cybersmart online helpline is a joint initiative with the Kids Helpline, and offers free, confidential advice and support from counsellors who are trained in listening to children and have cybersafety experience.
- Following a successful pilot of the *ThinkUKnow Australia* cybersafety program in Term 1, 2009, the AFP, in partnership with Microsoft and supported by ninemsn, launched the national roll-out of ThinkUKnow in February 2010.
  - The ThinkUKnow cybersafety program focuses on raising awareness of cyber safety and security risks by educating parents, carers and teachers. The ThinkUKnow presentations are delivered by trained AFP, Microsoft and ninemsn volunteers.
- DEEWR, in conjunction with educational communities from around Australia, has established the <http://bullyingnoway.com.au> website to provide information and advice on ways to combat bullying, violence, harassment and discrimination, and
- The National Framework for Protecting Australia's Children 2009-2020, developed by FaHCSIA for the Council of Australian Governments, recognises the importance of raising awareness about the role of the internet as a mechanism for the sexual abuse or exploitation of children and young people.

Initiatives in states/ territories include<sup>1</sup>:

- in the Northern Territory, a Safe Schools NT framework was established in 2007—the NT also recognises that indigenous cyber-bullying issues are a priority

---

<sup>1</sup> Based on information provided to the Cyber-bullying Sub-committee at its meetings of 24 November 2008, 31 August 2009 and 8 June 2010.

- in Queensland, protocols for student internet usage have been adopted by state schools—schools must also publish their Safe and Supportive Schools policy on their websites
- in South Australia, teachers have been trained in child protection and safety, including internet safety, and brochures were provided to schools in 2007 providing advice to parents in dealing with cyber-bullying—the SA approach has involved a coalition of state, Catholic and independent schools
- in Tasmania, a Kindergarten to Year 10 curriculum dealing with cybersafety has been developed—the Tasmanian Department of Education also has a website providing policy and information for teachers and students on cyber-bullying
- in Victoria, an educational channel to schools has been established which provides access only to ‘safe’ websites
- in Western Australia, the WA Department of Education and WA Police have established a working group to address curriculum, behaviour and technology issues as well as liaison with parents, and
- in New South Wales, during November 2009, the NSW Department of Education hosted a Cyberbullying Forum during November 2009 resulting in the establishment of new links between educators, researchers, industry experts, students, parents and community members. These links will facilitate collaboration on the development of strategies for the whole community to address cyber-bullying.

Industry has also taken significant steps to inform their customers about cybersafety threats, for example:

- Telstra has implemented a number of cybersafety activities, including parent and community cybersafety education programs, internet security education activities, and cooperation with law enforcement to eliminate anti-social online behaviour.
- Telstra has developed the BigPond Home Security Suite, a comprehensive security software package.
- MySpace Australia delivered an interactive cyber-bullying education campaign and competition for Australian high school students during March and early April 2009 in conjunction with SonyBMG, the Daily Telegraph, Kids Help Line and the NSW Education Department.
- Google delivers user education, technology tools such as SafeSearch Lock, and cooperates with law enforcement and industry partners. Over the past year, Google has worked with Australian child safety and wellbeing organisations to educate people about cybersafety. For example:
  - Australian Federal Police ThinkUKnow YouTube channel ([www.youtube.com.au/thinkuknowaus](http://www.youtube.com.au/thinkuknowaus))
  - Bravehearts YouTube channel for White Balloon Day ([www.youtube.com.au/bravehearts](http://www.youtube.com.au/bravehearts))
  - Smart Online, Safe Offline (SOSO) launch of an interactive cyber-bullying campaign, called Cyber-Bullying Affects Real Lives ([www.youtube.com.au/soso](http://www.youtube.com.au/soso))

- Google has also provided funding for a number of Australian child safety and wellbeing organisations: Kids Helpline, NAPCAN, Inspire Foundation, and The Alannah & Madeline Foundation.
- Microsoft has been working with Australian law enforcement authorities to roll out the Child Exploitation Tracking System (CETS) and other technological tools to help more effectively identify victims and track down online paedophiles.
- Microsoft is also involved in a range of partnerships including *ThinkUKnow* (with the AFP and Ninemsn), the *Smart Online Safe Offline* initiative (with the National Association for the Prevention of Child Abuse and Neglect—NAPCAN) and the Cybersafety and Wellbeing Initiative<sup>2</sup> (with The Alannah and Madeline Foundation).
- Microsoft provides Parental Controls, designed to put parents' minds at ease and give them confidence in their ability to manage what their children can do on the computer.
- Facebook, in addition to its participation in and support for numerous child safety initiatives around the world, has established a Facebook Global Safety Advisory Board comprised of five leading Internet safety organizations who serve in a consultative capacity to Facebook on issues related to online safety. They provide Facebook with the latest cyber safety information.
- Facebook has developed a Facebook Safety Center that provides users with easy to access safety information and specific resources for teens, parents, educators and law enforcers.
- Facebook has developed a Facebook Security Page to provide users with the latest cyber-security information as well as a complimentary 6 month subscription to McAfee security and antivirus software.
- Facebook has been working closely with the Australian Human Rights Commission on public initiatives to combat cyber-racism and hate.
- Facebook has worked closely with the Australian Attorney General and AFP to develop streamlined communications mechanisms to address situations where law enforcement is needed

Non government organisations are active in the field of cybersafety and child protection generally, for example:

- The Alannah and Madeline Foundation has developed a cybersafety and wellbeing framework for primary and secondary schools, promoting the smart, safe and responsible use of ICTs. Called The Cybersafety and Wellbeing Initiative (also known as eSmart), it provides links to relevant resources through an online portal, support for schools in implementing the framework, and an online system for tracking and reporting on progress through the framework. Schools that satisfy the requirements are acknowledged as 'eSmart' schools.
- Child Wise has a key role in the 'Speak Up' program which raises awareness of child abuse—the organisation also delivers child protection training workshops in Australia and the Asia Pacific Region.

---

<sup>2</sup> Formerly called the Cybersafety and Wellbeing Campaign.

- Bravehearts provides education programs and materials directly to children and young people through its school-based initiatives. Additionally, Bravehearts' website and social networking sites provide information and resources to young people and adults on cybersafety. The organisation runs workshops focussed on child sexual assault issues and risk management for a number of sectors. Bravehearts works in partnership with MySpace on the 'Respect MySpace' initiative, which provides information, education and awareness messages to users of MySpace who are at risk of sexual assault.
- The Australian Library and Information Association (ALIA) undertook the ALIA Internet Access in Public Libraries Survey 2008 that provides current information on how public library internet services are managed, delivered and used in responding libraries. The next survey is due to be undertaken in late 2010.
- The National Association for the Prevention of Child Abuse and Neglect (NAPCAN) delivered its Smart Online Safe Offline (SOSO) initiative in November 2009.

The CWG considers that education, awareness and assistance should continue to be a priority for the Government in terms of its cybersafety strategy. There is considerable value in Australian organisations and jurisdictions working more closely to ensure that cybersafety initiatives provide a consistent message. This is in keeping with trends in recent research that indicate that a coordinated approach to improving cybersafety and security brings significant benefits. The growing number of cybersafety initiatives being independently developed in Australia and overseas increases the risk that key safety messages may be diluted and that some products fail to maintain currency or deliver maximum effectiveness.

The CWG is developing an easy guide to cybersafety features of social networking and online game sites. The guides will make it easier for parents and children to see the cybersafety features available on popular social networking and online game sites. The guides are expected to be launch by the end of 2010.

The CWG considers there would be merit in establishing a central point (eg a website) through which teachers, parents and children can access information on the full range of cybersafety education initiatives being undertaken by different agencies and organisations. The ACMA's cybersafety website, launched in July 2009, significantly delivers on this by providing a single access point for cybersafety advice for children, parents, libraries and schools and also provides links to other stakeholder organisation that deal with particular aspects of cybersafety and security—including government, education, child welfare and advocacy and industry.

The website, *cybersmart.gov.au*, provides access to an online helpline for young people, contact details for the Kids Helpline services, and a reporting mechanism for people (the Cybersmart Online Helpline, provided in conjunction with Kids Helpline), with concerns about online contact or content. Advice from the Youth Advisory Group in 2009 regarding layout, content and promotion was used to inform the development of the website. The CWG will continue to closely monitor the implementation/ operation of this and other initiatives, to advise on how they might be made most effective.



The CWG has provided input into the development of a new government cybersafety initiative - the Cybersafety Help Button. The help button will provide internet users, particularly children, with easy online access to cybersafety information and assistance. The help button was developed from the advice received from the YAG who said they would like a 'one-stop shop' for cyber-safety advice and assistance. The button is expected to be launched to the public in September 2010.

The CWG will also consider overseas initiatives, to gauge their application to Australia. One such initiative is Cybermentors, which was launched in the United Kingdom on 3 March 2009.

In the coming year, CWG members will again actively consider ways to participate in and promote International Safer Internet Day 2011 which is held in February each year with Australian input coordinated by the ACMA.

### *Law enforcement*

Regulation and law enforcement is another critical strategy to combat cybersafety threats, for example:

- The ACMA regulates online content under the *Broadcasting Services Act 1992*, including issuing take-down notices to Australian hosts of prohibited content.
- The AFP investigates child exploitation offences involving the internet.
- Commonwealth and state and territory Attorney-General's departments administer legislation in relation to grooming and procuring offences — Commonwealth legislation complements state and territory grooming and procuring offences by targeting predatory behaviour that occurs through a carriage service.

The CWG acknowledges the effectiveness of the ACMA take-down regime and notes that since 1 January 2000 the ACMA has issued take-down notices in respect of over 370 items with no instances of non-compliance. The ACMA believes that these take-down arrangements, together with complementary criminal legislation, are a significant deterrent to hosting illegal content in Australia. The ACMA work in this area is a model that could usefully be adopted in other countries.

CWG members representing industry and non government organisations work actively with law enforcement authorities.

### *Technical measures*

The CWG recognises that while technology is a powerful tool in the protection of children and young people, it cannot provide a complete solution to the challenge of protecting young Australians from cybersafety threats. The CWG agrees that a strategy employing a range of tools including technology, education, and law enforcement is the most effective approach to creating a safe online environment.

The CWG has considered a range of new technologies to mitigate cybersafety risks, for example:

- MySpace uses a search algorithm to detect users who may be too young to register for the site, reviews images and videos, and hashes images identified as pornographic or sexually explicit to prevent subsequent upload.
- Google employs a range of measures to protect users of its services, including, on its YouTube service, technology which prevents the uploading of material previously removed for being contrary to the site's acceptable use policy.

- Microsoft provides home users with free downloadable security tools.
- Telstra has developed the BigPond Home Security Suite—a comprehensive security software package that provides protection from inappropriate content, spam, viruses, and phishing attacks. A subscription includes automatic updates and a 24 hour helpdesk service. The parental controls contained in the BigPond Security Suite allow parents to:
  - set time limits on their children's internet usage
  - monitor the sites their children visit and provide parent's with reports of their browsing history
  - block known problem sites and filter websites for inappropriate language, images and topics—all depending on each child's age group, and
  - tailor protection for their family and their PC using pre-set filters and flexible controls.
- Telstra is continuing to evaluate technologies which aim to enable the blocking of a defined blacklist of URLs and are sharing the results of their evaluations with the Government.
- Yahoo!7 has implemented technology and policies to help identify apparent child pornography violations on its network. These include using a combination of filters, algorithms, and human review, as well as user reports of abuse.
- Yahoo!7 has enabled a “SafeSearch” feature to prevent display of adult content in search queries made by that user’s Yahoo! account (turned on by default). Parents can lock SafeSearch on to prevent children from turning it off. On Yahoo!’s mobile service “oneseach”, all users default to SafeSearch mode and children registered as under 17 cannot turn the function off.
- Webshield and other small ISPs who have recently entered the market have implemented ISP level filtering services as part of their business model.
- Telstra, Optus and Primus have agreed to voluntarily filter child abuse material, and
- Similarly, overseas ISPs in the UK and Europe voluntarily filter content – in Germany the major search engine providers have voluntarily agreed to implement measures that reduce the risk of children inadvertently accessing certain types of content.

The CWG has considered the *Safer Social Networking Principles for the EU*, which establish a common set of rules concerning the protection of minors. The CWG considers that the approach taken in the EU provides a sound reference point for comparable measures that could be adopted by Australian social networking sites.

### *International Cooperation*

Given that the majority of internet sites that pose cybersafety risks are hosted overseas, the need for international cooperation in managing cybersafety risks is acute. Some countries are more receptive to cooperation than others. The CWG notes international cooperation is already taking place between some law enforcement authorities, and between organisations responsible for compiling website ‘blacklists’ and operating hotlines. The CWG acknowledges, in this respect, the ACMA’s membership of the International Association of Internet Hotlines (INHOPE). Member hotlines of INHOPE handle about 10 000 reports of illegal online content every month.

The CWG intends to explore the effectiveness of existing international co-operation measures and consider what more can be done to improve cooperation. One area deserving attention is how to replicate the benefits of the ACMA’s successful take-down regime across a wider range of countries. The CWG will therefore consider the current international co-operative arrangements for taking down child exploitation websites and advise on how they might be made more effective.

### *Work program for the next 12 months*

The CWG considers that its program of work for the next 12 months should concentrate on the cybersafety issues of:

- cyber-bullying
- contact (eg grooming), and
- privacy.

Strategies for effecting behaviour change in relation to each of these issues will be tailored to particular target groups, such as children of different ages, parents and teachers. Future strategies recommended by the CWG will be informed by lessons learned from earlier programs and strategies.

The CWG will provide further advice to Government regarding measures to counter cybersafety risks in the coming year. This advice will take into account the wide range of government, non-government and industry bodies already employing measures, as well as:

- commissioned (and other) research
- advice from the Youth Advisory Group on cybersafety, and
- overseas cybersafety initiatives and recommendations from key international reports on cybersafety.

In formulating cybersafety advice to Government, the CWG will seek to use baseline data drawn from the repeatable survey to track behaviour change over time in order to assess whether cybersafety strategies have been successful.

## **2. Background:**

The Minister for Broadband, Communications and the Digital Economy, Senator the Hon Stephen Conroy (the Minister), announced the establishment of an expanded Consultative Working Group on Cybersafety (CWG) in May 2008. The CWG is one of the initiatives of the Australian Government's \$125.8 million Cybersafety Plan, announced in the 2008-2009 Budget. A list of current CWG members may be found at [Attachment A](#).

The CWG is tasked with providing cybersafety advice to the Australian Government on best practice safeguards and priorities for action by government and industry. A copy of the CWG's terms of reference may be found at [Attachment B](#).

The CWG met regularly over the period between May 2008 and June 2010 and has established two CWG sub-committees: a digital age verification sub-committee and a cyber-bullying sub-committee. The former has met twice and the latter has met three times.

Secretariat support to the CWG is provided by the Department of Broadband, Communications and the Digital Economy (the Department).

## **3. Approach taken by the CWG**

Consultative Working Group (CWG) members come from a wide range of organisations with experience in cybersafety and social welfare issues. Information provided by members has highlighted the breadth of work being undertaken on cybersafety issues, both within Australia and overseas. However, the CWG acknowledges that more needs to be done.

The CWG notes the emergence of new research in the field of cybersafety that will help inform policy and will draw on such research when providing advice to the Minister in its next report. The CWG will also draw on advice from the Youth Advisory Group on cybersafety, which the CWG considers will be pivotal to obtaining the views of children and young people on:

- the nature of children's online engagement
- emerging cybersafety risks, and
- how best to tackle these risks.

The CWG has considered a number of existing Australian and overseas reports on cybersafety; a list of these may be found at [Attachment C](#). These reports confirm the view that there is no single panacea to cybersafety problems and that coordinated treatments, involving as many stakeholders as possible and a combination of technological and non technological measures are likely to be most effective.

The CWG will closely monitor the implementation of recommendations contained in these overseas reports to gauge their relevance for the Australian context.

#### **4. Findings to date and next steps**

The CWG's terms of reference specify six areas of focus for the Group. These are:

1. the online environment in which Australian children currently engage
2. the nature, prevalence and implications of cybersafety risks
3. Australian and international responses to current cybersafety risks
4. opportunities for cooperation across Australian stakeholders and with international stakeholders
5. information required to realise the potential for achieving and continuing world's best practice safeguards, and
6. ensuring that the CWG's deliberations take account of new technologies.

The CWG's preliminary findings on these six areas of study are discussed below.

##### **4.1 The online environment in which Australian children currently engage**

A variety of research and expert opinion informed the CWG's consideration of the online environment in which Australian children currently engage.

The Australian Communications and Media Authority's (ACMA's) 2007 study, *Media & Communications in Australian Families, Report of the Media & Society Research Project* provides a snapshot of how Australian families with children, at the time of the study, interacted with electronic media and communication. The study reported that:

- Australian families are technology rich: nine in ten have an internet connection and three-quarters have broadband (more likely in upper income brackets) while 95 per cent of them own a mobile phone(s)
- the internet now has a significant place in children's lives: 8-17 year olds spent on average about an hour and a quarter a day online
- one in five 8-17 year old children have a computer in their bedroom, half of which have an internet (mostly broadband) connection
- older teenagers spent almost five times longer on line than the younger children studied
- 8-11 year olds spent one minute on average messaging on their mobile phones per day compared to an average of half an hour for 15-17 year olds
- computer gaming peaked at 11 (80 per cent) and then declined to 60 percent of 17 year olds, although the time spent gaming was highest amongst the older age groups
- media preferences change with age, younger children prefer to watch TV or movies or play games while older teenagers spend more time on the phone or the internet, or playing recorded music
- boys are more likely to be gamers than girls, and spend more time than girls when doing so, but girls report using mobile phones more

- girls tend to use the internet to communicate whereas boys are more likely to use it for entertainment
- on average, 8-17 year olds spend about one and a quarter hours online a day—15-17 year olds spend two and a half hours per day
- from age 14 onwards, 70 per cent of the sample were engaged in some form of web authorship (including social networking sites), with girls more likely than boys to do so—70 per cent of girls aged 14-17 had a MySpace or similar profile, compared to 50 per cent of boys in the same age group
- almost all parents recognise the benefits to their children of engagement in media and communication activities, although they do have concerns, particularly about their child's use of the internet, and
- the ACMA's Click and Connect research builds on this research and provides further insights—see Section 4.5.

As noted above, those surveyed by the ACMA recognised the benefits of young people engaging online, including advancing their ability to engage with the digital economy. This is consistent with the findings of overseas studies which report that, overall, most online communication appears to be positive, with the benefits significantly outweighing the negatives (Livingstone & Helsper 2007, Tynes 2007). The importance of online communication/ social networking as a tool for developing young people's social relationships is also recognised in the literature (Tynes 2007, Boyd 2008). Additionally, the OECD Ministerial Meeting on the Future of the Internet Economy recognised that efforts to expand access to the internet need to continue (OECD 2008).

In Australia, Government initiatives intend precisely such expansion.

#### *The Government's 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 \$2.4 billion over seven years to:

- provide for new information and communication technology (ICT) equipment for all secondary schools with students in years 9 to 12 through the [National Secondary School Computer Fund](#)
- support the deployment of [high speed broadband](#) connections to Australian schools
- support systemic change to increase the level of ICT proficiency for teachers and school leaders across Australia to embed the use of ICT in teaching and learning and support the development of innovative projects and research that enable professional learning in the use of ICT
- 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

### *The National Broadband Network*

The Australian Government has established a company, NBN Co, to build and operate a new high speed National Broadband Network.

The new network will overcome the problem currently faced in Australia where broadband to homes and workplaces is delivered over an ageing copper-based network. The objective is to provide at least 90 per cent of homes, schools and workplaces with ‘fibre to the premise’ delivering speeds of 100 megabits per second and connecting all other premises with next generation wireless and satellite technologies, offering speeds of 12 megabits per second or more.

These initiatives will impact on the online environment in which Australian children engage; an environment that is already dynamic, requiring ongoing monitoring at both the domestic and international levels. Age, sex, technology, education, guardianship, access, user preferences and perceived benefit are the factors most likely to drive changes in children’s online engagement.

The CWG will continue to focus on factors influencing children’s online engagement. This will include consideration of domestic and international research on, and developments in, technology, education strategies, user preference, user guardianship and perception of benefits (see *Research* segment at [4.5](#)). It will also include consultation with young Australians through the Youth Advisory Group on Cybersafety (see *Consultation with Youth* segment at [4.5](#)).

## **4.2 The nature, prevalence and implications of cybersafety threats**

Empirical research in the field of cybersafety is comparatively limited, partly because it is a relatively new issue but also because it would be unethical to conduct experimental studies to gauge the harm from children’s exposure to, for example, pornography (ACMA 2007). Nevertheless, a number of surveys have been conducted in recent years and these, combined with research that does exist, allow preliminary trends to be deduced. These include:

- risks from the internet go hand in hand with benefits but that, generally, most online communication appears to be positive and benefits outweigh the risks (Livingstone & Helsper 2007; Tynes 2007)
- some children are at greater risk than others (Livingstone & Helsper, 2007)—vulnerable children, for example those with low life satisfaction and poorer family relationships, appear to be more at risk, as a general rule, and more likely to engage in risky online behaviour (ISTTF 2008)
- the risks children and young people face online are similar to those they face offline and young people often contribute to such problems (ISTTF 2008)
- there is a digital divide between many parents and their children (Livingstone & Bober 2005; EC 2007)—this can stem from parents being less computer literate than their children and the tendency for children to hide negative online experiences from their parents—possibly from fear that their access to the internet will be reduced or denied

- online experiences will never be risk free so that coordinated, relevant treatments to address risk, involving as many stakeholders as possible, may be the best strategy—a combination of technological and non technological measures is likely to work best (Byron, 2008; ISTTF 2008)
- piecemeal approaches to promoting online safety and security are less effective than more strategic and coordinated approaches (ISTTF 2008)
- exposure to harmful, problematic and illegal content is most likely to occur to those that seek it out, such as older male minors (ISTTF 2008)
- long-term harm from exposure to online pornography is more likely in young people who exhibit prior aggressive tendencies or behavioural disorders, or prior sexual or violent offending (Millwood Hargrave, A & Livingstone, S, 2006 cited in ACMA 2007)
- the ready availability and acceptance of pornography among young people means that efforts to restrict exposure needs to be accompanied by educational approaches that enable them to navigate toward a sexually healthy non violent adulthood (Bryant 2009)
- exposure to online pornography can foster ‘drifting’ behaviour, where young people develop an unhealthy curiosity about, and tolerance for, images of significant concern, such as child abuse, after initially viewing images that might only be regarded as inappropriate. (EC 2007)
- victims of harassment, and those that were depressed, find it harder to avoid unwanted exposure to internet pornography (Wolak et al 2007)
- video game overuse is most commonly seen among MMORPG players (massive multiplayer online role playing game), who can be somewhat marginalised socially (Khan 2007), and
- the percentage of young people receiving sexual solicitations online was 13% in 2006 with most recipients (81%) between 14-17 years of age, the vast majority of whom were female—most of those making the approach were also adolescents—a small percentage of solicitations result in offline contact and, for those that do, most victims are underage adolescents who know they are going to meet adults for sexual encounters (ISTTF 2008).

The CWG considers that while the cybersafety risks faced by Australian children impact differently across online communities, the nature and implications of risks such as:

- cyber-bullying
- inappropriate handling of one’s own and others’ private information
- exposure to and creation of inappropriate content
- computer gaming addictions, and
- sexual predation

are likely to be significant and present long-term negative implications for individual children, their families, their communities and Australia’s digital economy, including social and cultural norms.



The CWG intends to further explore the implications of these key risks on Australian children. This will include further consideration of domestic and international research, and consultation with young Australians through the Youth Advisory Group. Drawing from these sources, the CWG will review and refine key cybersafety messages and look to improve their promotion in the community. This will be undertaken in conjunction with key cyber security messages where appropriate. These messages will reflect behavioural changes sought of children, parents and teachers regarding cybersafety.

Cyber-bullying, which the CWG considers to be an issue of significant concern, is the specific focus of one of the CWG's two sub-committees. The CWG Cyber-bullying Sub-committee has identified and acknowledges the following key messages:

- the situation is not all bad—the internet is generally a positive place for children and young adults
- cyber-bullying exhibits the same basic characteristics and behaviour as conventional bullying
- strategies for dealing with face-to-face bullying are also effective for cyber-bullying
- there is still time in Australia to put strategies in place to prevent serious problems but action should be taken now
- young people need to be involved in developing solutions—their involvement means that measures undertaken are likely to be better accepted.
- cyber-bullying is a behavioural issue that needs to be dealt with by the wider community rather than just by schools
- there is a digital divide between parents and their children in terms of knowledge of the online environment
- it is important not to punish the victim by removing access to the internet when they report being cyber-bullied, and
- state educational authorities need to pursue coordinated responses to the problem of cyber-bullying.

The CWG considers that the sub-committee is an important means for education stakeholders from across jurisdictions, industry and child protection organisations to jointly consider and advise on initiatives to address cyber-bullying issues.

### **4.3 Australian and international responses to current cybersafety risks**

The CWG has considered many Australian and international responses to cybersafety risks. These include: education and information strategies, regulation and law enforcement, and industry commitment to safer social networking environments.

#### *Education, awareness and assistance*

The CWG recognises that education is a key part of any cybersafety program. Cybersafety education initiatives are being delivered by many stakeholders in Australia, including industry, governments (both federal and state/ territory), and non-government organisations.

The CWG considers that education, awareness and assistance should continue to be a priority for the Government in terms of its cybersafety strategy.

There is considerable value in Australian organisations and jurisdictions working more closely to ensure that cybersafety initiatives provide a consistent message. This is in keeping with trends in recent research that indicate that a coordinated approach to improving cybersafety and security brings significant benefits.

The CWG is of the view that there is merit in establishing a central point (eg a website) through which teachers, parents and children can access information on the full range of cybersafety education initiatives being undertaken by different agencies and organisations. The ACMA's Cybersmart website plays a crucial role in this regard, as does the ACMA online helpline. The CWG will continue to monitor the operation of these initiatives and advise on how they might be made more effective. Advice from the Youth Advisory Group will be important in this regard.

The CWG has provided input into the development of a new government cybersafety initiative - the Cybersafety Help Button. The help button will provide internet users, particularly children, with easy online access to cybersafety information and assistance. The help button was developed from the advice received from the YAG who said they would like a 'one-stop shop' for cyber-safety advice and assistance. The button is expected to be launched to the public in September 2010.

The CWG is developing an easy guide to cybersafety features of social networking and online game sites. The guides will make it easier for parents and children to see the cybersafety features available on popular social networking and online game sites. The guides are expected to be launch by the end of 2010.

#### *ACMA initiatives*

The ACMA provides a suite of cybersafety education initiatives, including cybersafety programs and resources for schools and outreach activities for students, parents and teachers. The ACMA's programs include professional development workshops for educators and general internet safety awareness presentations for teachers, parents and students. The ACMA also provides a range of online educational resources and programs which are available through the Cybersmart website ([www.cybersmart.gov.au](http://www.cybersmart.gov.au)).

The CWG intends to draw on the experience of individual CWG members and the views of the Youth Advisory Group to provide advice to the ACMA on how to ensure the relevance and currency of its cybersafety messages and resources.

#### *ACMA's Cybersafety Outreach program*

The ACMA's accredited professional development for educators program is a free one day workshop which covers a diverse range of issues including cyber-bullying, safe social networking, identity theft and exposure to inappropriate content and contact. It gives teachers hands-on experience in how to effectively use the ACMA's cybersafety educational resources, including lesson plans, interactive games and teaching guides. The aim of the program is to provide teachers with ready-made tools to engage students with cybersafety issues in the classroom teaching them skills and strategies to have safe online experiences. It also informs educators on the legal responsibilities of schools and teachers and looks at policies and processes to effectively manage cybersafety issues.

The professional development program has been accredited or endorsed in all states and territories across Australia.

A pre-service teacher program for student teachers in their final year at university was launched by the ACMA in June 2010. This trainee teacher program is aimed at equipping pre-service teachers with the skills and knowledge to educate their future students about cybersafety issues such as cyberbullying, sexting, safe social networking, e-security and identity protection.

The Outreach program also includes the delivery of Internet Safety Awareness presentations for, teachers, students and parents. These one hour presentations highlight key cybersafety issues and deliver important messages and practical advice on how to minimise cyber risks. Since January 2009 over 159,000 students, parents and teachers have attended an Internet Safety Awareness presentation.

#### *ACMA's Educational Resources*

- The Cybersmart website, launched in July 2009, acts as a one-stop shop for general cybersafety information and advice targeted to each of its specific audience groups: young children, kids, teens, parents, teachers and librarians. It incorporates the Schools' Gateway, a comprehensive age-based education resource for teachers, featuring interactive education resources, lessons plans, a guide to students' use of technology, and links to cybersafety policies and procedures from education jurisdictions throughout Australia. The website has attracted more than 260,000 unique visitors since its launch;
- Specific education resources include:
  - Hector's World –for younger children: this includes recently launched episodes relating to cyber-bullying and e-security
- Resources for primary and secondary students such as Cyberquoll, Cybernetrix and WiseuptoIT
  - Let's Fight it Together, a comprehensive resource for schools dealing with cyber-bullying, and
  - The Interactive Shared Learning program: this includes the very successful Cybersmart Detectives activity and the recently launched anti-cyber-bullying activity, Cybersmart Hero.
- The ACMA also operates the Cybersafety Contact Centre (1800 880 176), which provides assistance to those with general queries about cybersafety issues, bookings for Outreach presentations and ordering resources. In order to increase the likelihood that young people use the service, it has been expanded to include referrals made via SMS.

#### *Safer Internet Day*

The ACMA is the Australian co-ordinator for Safer Internet Day events and co-ordinated a range of activities for Safer Internet Day 2010, held on 9 February. Through its national cybersafety education program, Cybersmart, the ACMA marked the day with a series of internet safety events and activities including:

- a Cybersmart Detectives activity involving schools across Australia
- launching cybersafety-themed videos produced by children and young people on the Cybersmart website

- a ‘Hot Seat’ in children’s networking website SuperClubsPLUS Australia for upper primary and lower secondary school students, and
- a mailout to all Australian local councils and public libraries with Safer Internet Day posters and other cybersafety materials.

Safer Internet Day was used by the following groups to publicise or launch new cybersafety events and initiatives: the AFP, Google, Yahoo!7, MySpace, Microsoft, Interactive Games and Entertainment Association, Bravehearts, The Alannah and Madeline Foundation, Telstra, the Internet Industry Association, Mr Nick Abrahams, public libraries, Kids Helpline, state police and community technology centres.

The CWG notes that there needs to be an increase in public awareness of cybersafety issues generally. In the coming year, the CWG will examine options for participating in and promoting international Safer Internet Day 2011 which is held in February each year.

#### *Initiatives of other Australian Government bodies*

The CWG recognises the initiatives of other Australian Government agencies that touch on the issue of cybersafety, including:

- the National Framework for Protecting Australia’s Children 2009-2020, developed by FaHCSIA for the Council of Australian Governments, which recognises the importance of raising awareness about the role of the internet as a mechanism for the sexual abuse or exploitation of children and young people, and
- the Review of the National Safe Schools Framework being coordinated by DEEWR—the current framework, which has been in place since 2003, is being reviewed to, among other things, take into account the emergence of new technologies and, as a result, cyber bullying. The Review concluded in June 2010.

#### *Cybersafety initiatives of non-government CWG member organisations*

Child Wise activities to July 2009 include:

- planning assistance and delivery of workshops for the World Congress III Against Commercial Sexual Exploitation of Children and Adolescents
- a presentation on the prevention of child sex tourism to participants of the East Asia and the Pacific Preparatory Meeting for the World Congress
- child protection training workshops in Australia and the Asia Pacific Region supporting the Australian Government’s Child Protection Policy in relation to all overseas aid activities
- training workshops in Cambodia
- involvement in the ‘Speak Up’ program, which raises awareness of child abuse and encourages people to be proactive if they have concerns about a child.
- a National Child Abuse Helpline which provides free advice by telephone and online to people concerned about child sexual abuse.

Bravehearts, during the period 2008-2009, continued its partnership with the social networking site MySpace through the “Respect MySpace” initiative, which provides information, education and awareness messages to over 2 000 users of MySpace who are at risk of sexual assault, enabling them to access help and support. The Bravehearts MySpace page is monitored by a psychologist able to provide support to users seeking advice, and in some cases referrals. Bravehearts’ on-line presence has also been increased through the development of two Facebook pages.

The ‘Bravehearts Inc- Official Site’ has over 800 members and the ‘Make Australia the Safest Place to Raise a Child’ Cause page has over 5,000 members. Bravehearts:

- is focussed on creating further opportunities to partner with others to ensure smart and safe use of the internet;
- in line with this, provided content to Google for its relaunched Family Safety Centre.
- has forged relationships with law enforcement agencies in relation to strengthening responses to cyber-threats, and Bravehearts’ Founder was invited to speak on child protection at the 50<sup>th</sup> Management of Serious Crime Program.
- provides education programs and materials directly to children and young people through its school-based initiatives, and
- runs workshops (Supporting Hands) across a number of sectors specifically focussed on child sexual assault issues, and which include risk management.

The Alannah and Madeline Foundation announced the development of its Cybersafety and Wellbeing Initiative (also known as eSmart)<sup>3</sup> on 30 August 2008. The Initiative is a broad social change approach, acknowledging that cybersafety is the responsibility of the whole community; however the Foundation has focused on schools as the first priority setting. It is modelled on the SunSmart campaign which involved schools in changing attitudes through 'no hat, no play' and other sun smart policies that influenced student behaviour.

The Initiative’s *eSmart Schools Framework* is a proactive and strategic response to cybersafety concerns facing schools throughout Australia and promotes the smart, safe and responsible use of communications technologies.

Through an online portal schools access best practice cybersafety and wellbeing policies, curriculum, and whole-school change management guidelines. *eSmart* also highlights some examples of the best use of these technologies, and has the positive use of technology for teaching and learning as a core approach.

The Cybersafety and Wellbeing Initiative will connect teachers, parents, young people and the community to a wide range of expert resources, including those developed by the ACMA. The Initiative does not try to replicate the work of agencies such as the ACMA, but acts as a channel to their content. Importantly, *eSmart*’s system for tracking progress and reporting to achieve ‘*eSmart*’ status drives school implementation of cybersafety.

---

<sup>3</sup> Formerly called the *Cybersafety and Wellbeing Campaign*.

A national pilot of the *eSmart Schools Framework*, funded by the Department of Education, Employment and Workplace Relations, has recently been conducted in over 150 schools around the country, with positive feedback from participating schools. A final report on the outcomes of the pilot has been submitted to DEEWR. Consultation is ongoing with education jurisdictions and other stakeholders to ensure the Initiative aligns with a national standardised approach on how schools manage the smart use of communications technologies and the safety risks.

An important component of a successful behaviour change initiative to increase cybersafety within the community is a social marketing/advertising campaign akin to SunSmart's very successful "Slip Slop Slap" campaign. The design and development of this marketing campaign for eSmart has been completed by the social marketing company Shannon's Way, who also created the eSmart brand.

The Alannah and Madeline Foundation is already planning to extend eSmart beyond the school gate and with the Australian Library and Information Association (ALIA) has commenced work on eSmart Libraries.

The CWG has received a detailed presentation on the Cybersafety and Wellbeing Initiative and considers that it provides a solid framework for increasing awareness amongst teachers of the range of available cybersafety education resources and a system for guiding them to use the best available resources to ensure their school has in place effective cybersafety practices.

The Australian Library and Information Association (ALIA) is active in developing and promoting cybersafety policies and measures for all Australian libraries, particularly public and school libraries.

ALIA is active in the following ways:

- conducts regular surveys, with the next survey to be undertaken in late 2010, about internet access in public libraries which provide current information on how public library internet services are managed, delivered and used in responding libraries
- supports an expert advisory group to advise the Association which comprises ALIA members in public and educational libraries, academics and the information trade
- has a set of guidelines for libraries to ensure cybersafety for library users. The guidelines cover user behaviour policies, location of internet computers, customised web pages, collaboration with parents, and community education.
- works with the Australian Media and Communications Authority (ACMA) to assist library staff in promoting safe internet use in public libraries, particularly for children. Two guides were developed in 2008, and subsequently revised with ALIA's collaboration in 2009: *Cybersmart guide for library staff*, and the *Cybersmart guide for families*. The training videos for library staff, produced in 2008 by the ACMA with ALIA's assistance, continue to be promoted and used in public libraries <http://www.cybersmart.gov.au/Libraries.aspx>
- supports and promotes the Federal Government's National Cyber Security Awareness Week by providing advice about the most suitable resources for libraries, communication channels for engaging with the library community, and promoting print resources to libraries eg flyers, posters, bookmarks.

- supports and promotes the Federal Government's campaigns, Safer Internet Day and Stay Smart Online
- collaborates with ASLA (Australian School Library Association) as the other national peak body representing library workers in school libraries to promote cybersafety messages and to ensure that school library staff are familiar with cybersafety policies and measures
- is working with The Alannah and Madeline Foundation to extend the Foundation's e-smart schools program to e-smart libraries
- is a member of the Safer Internet Group which brings together Australia's leading sponsors of research, outreach and online safety campaigns to ensure that internet users, particularly children, have a safe experience online.

The National Association for the Prevention of Child Abuse and Neglect (NAPCAN) delivered its Smart Online Safe Offline (SOSO) initiative during the year. The Australian program of SOSO started as a one year pilot and then moved to a three year campaign.

The key points of SOSO in Australia to date have been "*People aren't always who they say they are*" and "*Don't give away too much information about yourself online*". Of the potential demographic of 2.4 million, some 1.57 million have visited the SOSO website since it commenced. The average visit lasted three minutes with four different interactions per average visit. The content of the campaign has been heavily driven from children's input, in order to determine what measures are likely to be successful. In Australia the SOSO project expects to commence a new campaign targeting cyber-bullying in the near future.

*Education strategies pursued/ partnered by industry*

#### Telstra

As Australia's largest Internet Service Provider Telstra plays a leading role in cybersafety. Telstra has been committed to providing relevant information, internet products and expertise for many years to customers so they are better equipped to exercise reasonable care and responsibility to achieve the best value from their online experience. We work with industry, government, community organisations and internet users to help to address evolving online risks.

Telstra is strongly committed to minimising risks that its customers face online, including exposure to inappropriate and illegal content, online predators, cyber-bullying, online scams and identity theft. This commitment is reflected in several areas of Telstra's operations including its retail product offerings and the Telstra Foundation's philanthropic programs.

In October 2008, Telstra created the new Officer of Internet Trust & Safety role within the company. CWG member, Darren Kane, was appointed to the position. Mr Kane also chairs Telstra's newly established Internet Trust and Safety Working Committee (ITSWC). The ITSWC is responsible for coordinating, across Telstra, a comprehensive approach to internet trust and safety.

Telstra has implemented a number of cybersafety activities, including parent and community cybersafety education programs, internet security education activities, and cooperation with law enforcement authorities to eliminate anti-social online behaviour. Additionally, the Telstra Foundation announced in 2007 a spotlight on cyber safety.

Providing \$3 million over three years the Telstra Foundation has supported *SuperClubsPLUS Australia*, a safe networking site for children, as well as other support programs and research that helps children and young people be safe online. These include a whole of community project in the Loddon Mallee region, a parent education and support program, a digital communication strategy aimed at young people, a youth led public debate on cyber safety and The Alannah and Madeline Foundation's Cybersafety and Wellbeing Initiative.

The Telstra Foundation announced in June 2009 a further commitment of \$3 million over three years to support its Spotlight on Cyber Safety funding program. This takes the total commitment to \$6 million over six years.

### MySpace

During March and early-April 2009 MySpace Australia delivered an interactive cyber-bullying education campaign and competition for Australian high school students through its website at [www.myspace.com/caughtinthecrowd](http://www.myspace.com/caughtinthecrowd). The campaign was run in conjunction with SonyBMG, the Daily Telegraph, Kids Help Line and the NSW Education Department to raise awareness on the issue of bullying at school, particularly from the viewpoint of a bystander or someone who passively contributes to bullying. Students were called-upon to produce a video to the vocal artist Kate Miller-Heidke's new single '*Caught in the Crowd*', a song about Miller-Heike's own high-school experience with bullying. There were in excess of 30 entries to the competition and the standard of production was generally very high. The winning entrant won a performance from Kate at their school (Upper Coomera State College, QLD) and \$2 000 worth of Sony hardware for the school. Feedback from teachers who got involved with the promotion was very encouraging, with some teachers reporting their intention to use their school's video entry as an ongoing part of their wider anti-bullying education strategies. The *Caught in the Crowd* profile has been befriended by over 1 000 people and the videos from the campaign have had over 20 000 plays.

MySpace Australia also continues its partnership with the popular local teenage publication Girlfriend Magazine with the 'I delete bullies' campaign. To date, the profile has been befriended by over 10 000 Australians. This campaign, with ongoing online and magazine editorial, aims to educate young Australians about their options to minimise the ability for bullies to target them online, including blocking, deleting and reporting bullies.

### Microsoft

Microsoft Australia takes a global multi-pronged approach to cybersafety. This includes the development of technological tools, the strengthening of legislation, law enforcement training and capacity-building and consumer education initiatives. Specifically, Microsoft is working with Australian law enforcement authorities to roll out the Child Exploitation Tracking System (CETS) and other technological tools to help more effectively identify victims and track down online paedophiles.

Globally, Microsoft has been working with law enforcement agencies, child protection groups and ISPs to look at what can be done via technology to help reduce the spread of child pornography, help track and trace on-line predators and educate the community about what can be done to protect children online.



The technology, called [PhotoDNA](#), was initially created by Microsoft Research, to help US based [National Center for Missing & Exploited Children](#) (NCMEC) in its efforts to find hidden copies of the worst images of child sexual exploitation known today. Once NCMEC assigns [PhotoDNA](#) signatures to known images of abuse, those signatures can be shared with online service providers, who can match them against the hashes of photos on their own services, find copies of the same photos and remove them. Also, by identifying previously “invisible” copies of identified photos, law enforcement may get new leads to help track down the perpetrators.

Microsoft is also involved in a range of partnerships including *ThinkUKnow* (with the AFP and Ninemsn), SOSO (with NAPCAN) and the Cybersafety and Wellbeing Initiative (with The Alannah and Madeline Foundation). Microsoft’s local online safety site is found at: [www.microsoft.com.au/protect](http://www.microsoft.com.au/protect). Earlier this year, Microsoft Australia also commissioned ‘For Safety’s Sake’ research. The survey found two thirds of Australian parents are concerned about the safety of their kids online, and more than 60 percent of parents allow their children to surf the net unsupervised and unrestricted at home.

One fifth of all Australian parents surveyed have caught their children looking at unsavoury material online, almost one third have found their children chatting to strangers, 36 percent have caught their kids downloading software without permission and another 12 percent have found their children handing over personal details. Two thirds of parents surveyed allowed their children free reign to the web at home, however, most believed that online danger is more likely to occur at a friend’s house (52 percent).

The survey revealed that in spite of concerns for online safety we could do much more to educate and help protect our children.

### Google

- Google has launched an online safety resource, Tips for Online Safety ([www.google.com/familysafety](http://www.google.com/familysafety)), which offers resources for families on how to use Google safely, and quick links to tools like SafeSearch.
- Through Google’s product Help Centres, it provides users with tips and articles for staying safe and protecting their privacy while using Google products. Google also invites its users to report illegal content or abuse they encounter on the web or in Google products through its Help Centres.
- In Australia Google supports non-profit organisations including The National Association for Prevention of Child Abuse and Neglect (NAPCAN), Inspire Foundation, The Alannah and Madeline Foundation, Kids Helpline and Bravehearts, to provide online public service announcements that promote access to resources about safety and other educational efforts. Google actively supports their efforts to raise awareness of child safety issues.

Google also works with law enforcement and industry in the following ways:

- Uses databases from designated organisations listing websites suspected of containing child sexual abuse images in order to remove illegal URLs from its search results.
- When it discovers child pornography or is made aware of it, Google responds quickly to remove and report it to the National Center for Missing and Exploited Children (NCMEC) or the appropriate law enforcement authorities.

- Google cooperates with child safety investigations, and has a legal team devoted to this effort.

### Facebook

- In addition to its participation in and support for numerous child safety initiatives around the world, Facebook has established a *Facebook Global Safety Advisory Board* comprised of five leading Internet safety organizations who serve in a consultative capacity to Facebook on issues related to online safety. They provide Facebook with the latest cyber safety information.
- Facebook has developed a *Facebook Safety Center* that provides users with easy to access safety information and specific resources for teens, parents, educators and law enforcers.
- Facebook has developed a *Facebook Security Page* to provide users with the latest cyber-security information as well as a complimentary 6 month subscription to McAfee security and antivirus software.
- Facebook has been working closely with the Australian Human Rights Commission on public initiatives to combat cyber-racism and hate.
- Facebook has worked closely with the Australian Attorney General and AFP to develop streamlined communications mechanisms to address situations where law enforcement is needed

### *Regulation and Law Enforcement*

The CWG considers appropriate regulation and law enforcement to have a key role in the mitigation of cybersafety risks. The regulation of online content by the ACMA, and investigation and prosecution of child exploitation offences by law enforcement authorities, are some of the key measures.

### *ACMA Regulation of Online Content*

Schedule 7 of the *Broadcasting Services Act 1992* requires content service providers to remove or restrict access to potentially prohibited content hosted in Australia by 6 pm the next business day, following receipt of an interim take-down notice from ACMA. Since 1 January 2000, the ACMA has issued take-down notices directing the removal of over 370 items of prohibited content from Australian internet sites, with no instances of non-compliance. Approximately half of these items concerned child abuse or child sexual exploitation material. There have been no instances of non-compliance with the take-down scheme to date. In 2009–10, the ACMA received only a handful of complaints about prohibited content hosted in Australia. The ACMA believes that these take-down arrangements, together with complementary criminal legislation, are a significant deterrent to hosting illegal content in Australia.

### *AFP investigations and initiatives*

The AFP's High Tech Crime Operations (HTCO) portfolio provides the AFP with an enhanced capability to combat technology enabled crime and to facilitate centrally-coordinated high technology operations support. HTCO prevents, detects, investigates and prosecutes technology crime across all areas of AFP policing.

Particular emphasis is placed on online child exploitation, including working closely with state and territory police and international law enforcement partners to combat offences against the exploitation and abuse of children online.

Through the Virtual Global Taskforce, the AFP works alongside its international law enforcement partners in joint investigations to infiltrate and shut down criminal groups involved in the commercial distribution of child exploitation material.

Examples of recent operational outcomes are:

An investigation into suspects involved in online sexual exploitation, contact offending against children and child sex tourism. Aspects of the investigation were conducted in partnership with the New South Wales Police Force. The investigation was significant in that offences spanned online exploitation, contact offending and child sex tourism.

No of Charges: 10

No of Arrests: 7

A 'mass' referral from Luxemburg: as at April 2010, there have been 1768 unique Australia-based Internet Protocol addresses identified which accessed a child sexual exploitation site on 7850 occasions. A total of 726 suspects have been identified and are currently being referred to AFP investigation teams and state/territory agencies. This operation is indicative of the enormous resource impact on the AFP of such mass referrals.

From January 2009 to December 2009 there have been 88 arrests and 118 charges for child sex offences – online child sex exploitation.

The use of peer to peer technology by offenders is especially challenging for law enforcement authorities, given that users do not go through ISPs. AFP investigations indicate that the majority of offenders are: male between the ages of 18 and 45 years; from various walks of life; and tend to drift into contact offences. The AFP note that it is harder to catch the propagators of online child exploitation material than the users of it.

The development of prevention strategies is critical to the AFP's work. Through the AFP's HTCOC Crime Prevention Team a number of crime prevention strategies have been developed and implemented to raise awareness of cybersafety and security. The Team has delivered over 110 primary and secondary school presentations during 2009-10. This includes an outreach to over 15,000 students, predominantly in New South Wales and the ACT.

Through programs such as *ThinkUKnow* the AFP, in conjunction with Microsoft, is able to provide an educative framework targeted at parents, teachers and carers to keep children safe online. Following the successful evaluation of the ThinkUKnow cybersafety program conducted by the Australian National University, ThinkUKnow was rolled out nationally commencing in February 2010.

As of June 2010, close to 200 schools across Australia have submitted an Expression of Interest for a ThinkUKnow presentation to be delivered at their school.

The AFP employs a Youth Advisor embedded within the Crime Prevention Team to assist with strategies to target youth online. This ensures that police, including the AFP Internet Policing Team, are able to operate in a contemporary environment. The Internet Policing Team engage in covert policing online to locate persons attempting to or engaging with youth online for the purposes of 'grooming' for sexual gratification.

The AFP's Victim Identification Team analyse images located during police operations in an attempt to identify children who have been abused or exploited online, including the identification of new images. The AFP has seized millions of images and videos of child exploitation material from investigations.

The CWG notes the significant increase in AFP activity to deal with cybersafety issues following the allocation of additional funding. The CWG will continue to monitor these trends and receive briefings from the AFP representative on the CWG, to enable the Group to advise on additional measures that the Government might consider.

#### *Commonwealth, State and Territory grooming and procuring offences*

Online grooming refers to a range of behaviour that is designed to make it easier for an offender to procure a child for sexual activity. For example, the offender might build a relationship of trust with a child, and then seek to sexualise that relationship (for example, by encouraging romantic feelings or exposing the child to sexual concepts through pornography).

Responsibility for combating child sexual exploitation is shared between the Commonwealth, States and Territories. States and Territories are generally responsible for child sex-related offences occurring domestically (eg within each jurisdiction). Traditionally, the Commonwealth has enacted child sex-related offences occurring across or outside Australian jurisdictions (eg, child sex tourism offences and offences involving the use of the Internet).

The Commonwealth first enacted offences targeting the use of a carriage service (ie the Internet or mobile telephone) for sexual activity with children, including grooming and procuring, in 1995. These offences were recently enhanced as a result of reforms to Commonwealth child sex-related offences, contained in the *Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010*, which entered into force on 15 April 2010.

The Act has improved the operation of Commonwealth online grooming offences, including by increasing penalties. The online grooming offence regime now covers the following offences:

- using a carriage service to transmit a communication with the intention of procuring a person who is, or who the sender believes to be, under 16 years of age to engage in sexual activity (procuring) – maximum penalty: 15 years imprisonment
- using a carriage service to transmit a communication with the intention of making it easier to procure a person who is, or who the sender believes to be, under 16 years of age to engage in sexual activity (grooming) – maximum penalty: 12 years imprisonment, and
- using a carriage service to transmit an indecent communication to a person who is, or who the sender believes to be, under 16 years of age – maximum penalty: 7 years imprisonment.

The Act has also introduced a range of new offences directed at online child sexual exploitation. These include:

- an aggravated offence directed at online child pornography networks, which is subject to the high penalty of 25 years imprisonment

- an offence criminalising the use of a carriage service to transmit indecent communications to a child, which carries a maximum penalty of seven years imprisonment, and
- a new offence of using a carriage service for sexual activity with a child, which carries a maximum penalty of 15 years imprisonment.

The new legislation also raises maximum penalties for existing online child pornography and child abuse material offences from 10 to 15 years imprisonment.

This legislation will support the Australian Federal Police (AFP), who play a significant role in ensuring children and young people are safe, whether in a real or virtual environment.

### *Industry Initiatives*

#### Internet Industry Association (IIA)

Industry codes can be developed by industry bodies and associations that represent sections of the content industry. The codes are developed by industry bodies under Schedule 7 of the *Broadcasting Services Act 1992* and can be presented to the ACMA for registration.

The IIA has developed industry codes covering online content, interactive gambling and online content services to help industry comply with the law at a practical level. Most recently, the IIA developed a new code of practice for online and mobile service content providers which took effect from 16 July 2008. The ACMA monitors compliance with the IIA Codes; members of the public can direct complaints about non-compliance to the ACMA.

The IIA has also developed a voluntary ISP Cyber Security Code of Practice (known as ‘the icode’) which is due to come into effect on 1 December 2010. The code is designed to provide a consistent approach for Australian ISPs to help inform, educate and protect their customers in relation to cyber security. It provides ISPs with a set of actions that they can take to help their customers to fix compromised computers. The code builds on the existing Australian Internet Security Initiative run by the ACMA, which assists ISPs to identify compromised customer machines on their networks. The operation of the code will be reviewed after 12 months.

The IIA ‘Family Friendly ISP Seal Program’ provides a visible symbol, the ‘Ladybird Seal’, to show which Australian ISPs are compliant with the IIA Codes. The IIA will take steps against a non-compliant ISP who bears the seal of compliance, in breach of its undertaking to comply. This can include terminating the license agreement which gives permission to use the seal.

#### Australian Mobile Telecommunications Association (AMTA)

AMTA and mobile telecommunications industry takes measures to minimise the risks associated with the misuse of mobile technology. On behalf of the mobile industry - AMTA’s approach to cybersafety is based on an acceptance of its community responsibility, a commitment to a whole-community approach, partnerships, practical advice and education and awareness.

AMTA has developed a website designed specifically for children which offers simple advice and includes links to a range of cybersafety sites. A range of materials have been developed, including a schools policy template to set practical rules for students, teachers and parents for the responsible use of mobile phones in school

environments. The template can be used as a starting point to assist the development of a school-based mobile phone use policy, which sets out the expectations and responsibilities of students, parents and teachers. It's adaptable to allow schools to add, delete or modify items to reflect the specific needs and standards of individual schools.

AMTA's tips on preventing cyber bullying for young people and companion advice for their parents and teachers have been promoted and circulated widely to schools, parents, education departments and community groups. For example, a guide for students called: "Mobile phones and bullying: what you need to know to get the bullies off your back" is also accompanied by a guide for parents and teachers to assist the victims of such stressful and distressing experiences.

#### *Industry Commitment to Safer Social Networking Sites*

In Europe and the United States, major social networking sites have entered into agreements on common rules and principles for the protection of young people using their sites. Copies of these agreements are at Attachment D. The CWG has been advised that, to the extent that the participating social networking sites operate on a global basis, the benefits of this agreement flow through to Australian users.

The *Safer Social Networking Principles for the EU* were signed by all major social networking sites active in Europe on 10 February 2009—Safer Internet Day. The Principles, which are non binding, establish a common set of rules concerning the protection of minors. Bebo, Facebook, Google/ YouTube, Microsoft Europe, MySpace<sup>4</sup>, Habbo Hotel and Yahoo! Europe are among the signatories to the agreement<sup>5</sup> and agreed to support the following seven principles:

- i. Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner.
- ii. Work towards ensuring that services are age-appropriate for the intended audience.
- iii. Empower users through tools and technology.
- iv. Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service.
- v. Respond to notifications of illegal content or conduct.
- vi. Enable and encourage users to employ a safe approach to personal information and privacy.
- vii. Assess the means for reviewing illegal or prohibited content/conduct.

In terms of practical application,<sup>6</sup> the principles recommend a range of good practice approaches which can help achieve safer social networking. Whilst acknowledging that one size will not fit all, these include:

---

<sup>4</sup> MySpace believes that the EU Principles provide a good model for Australia and notes that they have been adopted by the major social networking sites operating throughout Europe and in the Australian market.

<sup>5</sup> Compliance with the EU Principles mean that social networking services with a global reach extend to users worldwide, including in Australia.

<sup>6</sup> EU Principles:

[http://ec.europa.eu/information\\_society/activities/social\\_networking/docs/sn\\_principles.pdf](http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf)

"The document outlines the principles by which SNS providers should be guided as they seek to help minimise potential harm to children and young people, and recommends a range of good practice

- providing an easy to use and accessible "report abuse" button, thereby allowing users to report inappropriate contact from or conduct by another user with one click
- taking steps to ensure that the full online profiles and contact lists of website users who are registered as under 18 are set to "private" by default. This will make it harder for people with bad intentions to get in touch with a young person
- taking steps to ensure that private profiles of users under the age of 18 are not searchable (on the websites or via search engines)
- making privacy options prominent and accessible at all times, so that users can easily work out if just their friends, or the entire world, can see what they post online, and
- taking steps to prevent under-age users from using their services.

The United States entered into agreements with MySpace and Facebook in the first half of 2008. The US agreements are of a more prescriptive and binding nature than the EU Principles agreement. They list a number of principles against which MySpace and Facebook commit to certain actions, including establishing the ISTTF<sup>7</sup> which reported in December 2008. The organisations also commit to design and functionality changes, such as 'age locking' to prevent minors from changing their age to pretend to be older than they are, or adults changing their age to appear to be minors.

The CWG considers that the approach taken in the EU provides a comparative model for Australia and notes that there may be locally-based social networking sites which could usefully consider adopting such principles. The CWG was advised by the IIA that it will act to encourage such Australian sites to ensure they operate in a manner consistent with the EU principles. This will be complemented by the CWG's development of an easy guide to cybersafety features of social networking and online game sites.

#### **4.4 Opportunities for cooperation across Australian stakeholders and with international stakeholders**

The CWG, in considering a vast array of cybersafety material, finds that there is need for Australian agencies and jurisdictions to work together to ensure that cybersafety messages are consistent and effective. The growing number of cybersafety initiatives being independently developed in Australia and overseas increases the risk that key safety messages may be diluted and that some products fail to maintain currency or deliver maximum effectiveness.

---

approaches which can help achieve those principles. The guidance is not intended as a 'one size fits all' solution. It is recognized that the communications and internet industry is very diverse and ranges from large global providers to smaller locally run services. SNSs vary greatly in terms of the type of service, the platforms on which they can be consumed, their user demographics, the markets in which they operate and the jurisdictions in which they are based. All of these factors affect the levels and types of risks that are attendant to those services and the strategies that may be appropriate and reasonable to address such risks. Accordingly, in determining their own safety strategies, providers supporting these principles take into account the particular nature of their services in order to apply the relevant recommendations of these Principles. Therefore, while providers will support all seven Principles, it is for each provider to judge where and how far to apply the document's specific recommendations. These Principles are aspirational and not prescriptive or legally binding, but are offered to service providers with a strong recommendation for their use."

<sup>7</sup> Internet Safety Technical Task Force (US).

The large number of cybersafety initiatives could also result in a measure of overlap and the CWG considers that there are efficiencies to be made in rationalising effort. A list of some of the known Australian initiatives may be found at [Attachment E](#).

The need for cooperation amongst stakeholders was recognised by the ISTTF (2008) which considered that

*“All stakeholders must continue to work in a cooperative and collaborative manner, sharing information and ideas to achieve the common goal of making the Internet as safe as possible for minors.”* (page 6)

Coordinated effort and enhanced cooperation in relation to cybersafety activities is an area of priority for the CWG in its second year. The CWG notes that in the United Kingdom, the Government accepted a recommendation by the Byron Review (Byron 2008) to establish a single body to oversee a coordinated approach to the development and deployment of online safety initiatives.

Internationally, the CWG notes cooperation through the sharing of website ‘blacklists’, such as with the Internet Watch Foundation, and through multilateral bodies such as the Organisation for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC).

The ACMA is a member of the International Association of Internet Hotlines (INHOPE). INHOPE members must be able to take-down, or otherwise deal with, material on the internet that is illegal under local law. INHOPE member hotlines handle over 20 000 reports of illegal online content every month.

INHOPE has 40 member hotlines in 35 countries and is looking to expand membership into countries known to host significant amounts of online child exploitation material. INHOPE members have observed that illegal material can be more persistent in countries where legal frameworks for dealing with child sexual abuse and its depiction online are less developed.

Websites providing access to child exploitation material regularly change host location to avoid detection and removal. INHOPE member hotlines are well placed to collect information on the hosting location of such websites. In 2009, INHOPE launched a new reporting database for members that will streamline the referral of content from one member to another, and also help to reduce ‘double-handling’ of URLs by multiple hotlines.

During 2009-10, INHOPE members formulated a proposal to the Internet Corporation for Assigned Names and Numbers that would see action taken by domain name management authorities to ‘disable’ internet domains used to commercially distribute child sexual abuse material.

Opportunities also exist for international cooperation involving industry. For example Telstra (CWG member, Mr Darren Kane) was invited to give a presentation on internet content filtering at INTERPOL’s Crimes against Children Working Party Conference in June 2009. Due to extenuating circumstances, the conference has been deferred twice and is now due to take place in Lyon, France, in September 2010.

The CWG will seek to identify other priorities for Australia’s international cooperation efforts.



#### **4.5 Information required to realise the potential for achieving and continuing world's best practice safeguards**

The CWG intends to inform itself further on core information necessary for maintaining effective cybersafety strategies. The CWG has considered a range of contemporary research and survey material on cybersafety issues and is aware that a number of further studies are underway.

##### Research

###### *Children's cultural and leisure activities survey*

During 2008 and early 2009, the Department worked with the Australian Bureau of Statistics to incorporate a number of questions on cybersafety into the Bureau's Children's Participation in Cultural and Leisure Activities (CPCLA) survey. The survey collected information on children aged 5-14 years regarding their sporting and cultural activities, including online activities and those involving mobile phones.

The survey asked, for example, how the children are using the internet, where they use it, the types of activities they use it for (for example email, chat rooms, online games, listening and downloading music, educational research etc) and how many hours a weeks they usually access the internet at home. The survey also included questions about cybersafety practices, such as whether parents have installed an internet content filter, supervised their child's online activity, or educated their child about the safe and appropriate use of the internet.

With regard to the child's use of mobile phones, the survey sought information on whether they have one, and whether they use it for contacting family or friends or to access the internet. The survey also gauged whether the child has received bullying phone calls or text messages and whether his/ her parents have put safety measures in place, such as blocking phone numbers or restricting services, or educating the child about the safe and appropriate use of mobile phones.

The Bureau survey was conducted in April 2009. Findings were published in the *Household Use of Information Technology* report published 16 December 2009 The findings were that:

- 77% of all Australia's 1.5 million children had a computer in a public area of the house, 47% of children (927 000) had an internet content filter, 89% (1.8million) had their internet use supervised or monitored and 83% (1.6million) had been educated about safe and appropriate use of the internet.
- For the first three factors, birthplace of parents was a significant issue, with parents born in a non English speaking country less likely to have a computer in a public area, have a content filter or supervise internet usage.
- 3% of children (72 000) had experienced a personal safety or security problem with the internet. For this group, considering the most recent problem, just under half (33 000) had access to inappropriate material, one fifth (15 000) had strangers seeking personal information and one fifth (15 000) experienced threatening or bullying behaviour.
- 22% of children (182 000) with a mobile phone had restrictions on phone numbers or services, 53% (445 000) had their activities monitored and 81% (683 000) had been educated about safe and appropriate use of mobile phones.

- 3% of children (28 000) had experienced a safety or security problem with a mobile phone. Considering the most recent problem, nearly half (12 000) had experienced bullying or threatening behaviour, one third (9000) had received inappropriate material in a text or media message and 10% (3000) had strangers seeking personal information.

#### *Cybersafety Plan research - Review of existing research*

Following an open tender process, Edith Cowan University undertook a review and analysis of existing Australian and international research on cybersafety. The review provides a useful basis for future research.

#### *Repeatable survey*

Following an open tender process, IRIS Research was commissioned to undertake two repeatable surveys to collect information from parents, carers and educators on cybersafety and cyber security issues, including solutions and priorities for action. IRIS has developed the methodology for both surveys, and will be reporting on the results by September 2010. The intention of the surveys is to enable Government to:

- quantify and qualify cybersafety risks
- update its cybersafety policies
- inform program evaluation methodology, and
- operate effective communication strategies.

The CWG was briefed on the scope and methodology of the repeatable surveys, to maximise its alignment with the CWG terms of reference. The CWG notes that the Department has worked to ensure that, as far as possible, the surveys do not duplicate those being conducted by the Australian Bureau of Statistics or the ACMA. To this end, the surveys focus on the views of parents, carers and educators and are collecting data on:

- the online environment in which Australian children engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles)
- the nature of online engagement including frequency of use, time spent online, activities in which the child is engaged
- the prevalence of cybersafety and cyber security risks, including cyber-bullying, exposure to illegal and inappropriate content and breaches of privacy current responses to cybersafety and cyber security risks including:
  - the use of technical, educational and behavioural measures, and
  - awareness and use of Government cybersafety and cyber security initiatives
- the effectiveness of measures undertaken in response to cybersafety and cyber security risks

#### *ACMA Research*

In 2008, the ACMA commissioned a research project to explore children's use of social networking services, and their perceptions – and those of their parents - , young people's and parent's of online risks and opportunities. The research focused on the ways in which children and young people protect themselves online and the strategies they use to minimise online risk.

The research used a mixed qualitative and quantitative approach, with the qualitative phase comprising:

- four group discussions with young people aged 13-17 years
- two group discussions with parents of this age group
- eight ‘friendship’ triads with children aged 8-12 years followed by paired in-depth interviews with their parents and
- two bulletin boards with teenagers aged 13-17 years.

The quantitative phase of the report comprised 819 online surveys among children aged 8-17 years and their parents, with questionnaires tailored according to the audience.

Key findings of the *Click and Connect* reports were as follows:

- Children and young people have a high level of awareness of cybersafety risks and the key messages for staying safe online.
- For example, 75 per cent of children surveyed claim they know not to give out their address or phone number online and remember key safety messages such as ‘people aren’t always who they say they are online’.
- The internet is part of children and young people’s everyday lives, and as they approach high school, it is increasingly important to their social lives. Up to 97 per cent of 16 to 17 year olds claim to use at least one social networking service.
- Most young people are using online technologies as a way to connect with their real world friends, with a small proportion—17 per cent of 12 to 17 year olds—using online social networking to build networks of new friends.

The research findings, which were published in July 2009, have helped inform the ACMA’s delivery of cybersafety activities.

The ACMA published a survey on 10 March 2009 entitled *Australia in the Digital Economy: Trust and Confidence*. The survey, which was conducted nationally, gauged consumer attitudes and behaviour relating to online security (the report of the survey findings also includes a section on cybersafety). The report examines Australian internet users’ levels of trust and confidence in the internet and the factors which may build or inhibit that confidence.

The ACMA has also published three reports in its three year program of research examining developments in cybersafety initiatives internationally (including but not limited to, filtering technologies) aimed at protecting both young people and adults who access content on the internet. These reports, produced pursuant to a Ministerial direction, provide a comprehensive analysis of the evolution of online risk, exploring a wide range of measures that can be deployed to mitigate online risk and promote online safety.

#### *Other Australian research*

The reports of four major studies in the field of cyber-bullying have been published or are in train:

1. a national study into covert bullying, undertaken by Professor Cross of Edith Cowan University (ECU)—the *Australian Covert Bullying Prevalence Study* (2009), funded by DEEWR

2. a study on covert bullying undertaken by the University of South Australia and Flinders University—*Behind the Scenes: Insight into the Human Dimension of Covert Bullying* (2009), also funded by DEEWR
3. a Cyber-Friendly Schools Study conducted in 2007-08, which canvassed opinions/experience from staff and principals, and a Cyber-Friendly Student Summit project that is currently underway and which has a student focus, and
4. a Family Cyber Intervention trial, focusing on parents and libraries, which will be conducted in 2009-10—a five year randomised control trial will follow, in order to determine longer term changes in attitudes/awareness.

Edith Cowan University is also developing anti-bullying campaign information targeting rural areas and Aboriginal communities.

The CWG will also review other recent research including:

- the Australian Institute of Criminology report, *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences*.

#### *International Research*

The US Federal Communications Commission (FCC) has announced an inquiry into parental control technologies for video or audio programming. The inquiry will be undertaken as part of the FCC's implementation of the US Child Safe Viewing Act. The FCC has invited parents and children's advocates to advise the Commission on what tools they believe parents need in order to protect their children from content they deem harmful. Industry players have been invited to advise the Commission on what steps their organisations can take to help parents.

The European Commission's (EC's) study *Safer Internet for Children, Qualitative Study in 29 European Counties Summary Report* (2007) has generated the commissioning of two further European research projects. These are:

- the EC commissioned Flash Eurobarometer survey 2008, *Towards a Safer Use of the Internet for children in the EU—a parents' perspective*, which was published in December 2008
  - as the title suggests, the survey was conducted in order to find out parents' perceptions of their children's internet usage and potential risks they could face online, and
- the *EU Kids Online* series, a three year collaboration examining research carried out in 18 member states of the European Union into how children and young people use the internet and new media, which was published in June 2009
  - the project aimed to identify comparable research findings across Europe and to evaluate the social, cultural and regulatory influences affecting both risks and children's and parents' responses to them, in order to inform policy.

#### *Youth Advisory Group on Cybersafety*

The Australian Government's Youth Advisory Group on (YAG) Cybersafety was established in 2009. The YAG provides a forum where young people can talk directly to the Government about cybersafety. In its first year, the YAG consisted of 304 secondary students from 15 schools nationally. Over 12 200 posts on 865 topics were generated on *y@g Online*. Of those, over 5600 posts and 380 topics were cybersafety related.

The 2009 YAG provided advice to the Government on cybersafety issues such as cyber-bullying, mobile phone safety, privacy and online computer games from the perspective of young people. This advice led to the Government announcing two important initiatives aimed at keeping children safe in the digital world - the Cybersafety Help Button and the Teachers and Parents Advisory Group on Cybersafety.

The expansion of the ACMA's cybersafety education, awareness-raising and counselling services was also informed by feedback provided by the YAG. The ACMA's *Cybersmart* website and online helpline implemented a number of features consistent with initial advice from the YAG.

The 2010 YAG has expanded to include 500 primary and secondary students aged 8-17 years from 30 schools nationally. This group continues to provide advice to the government on cybersafety issues through the *y@g Online* site and face-to-face meetings. A small number of YAG members are also invited to present their key cybersafety messages in person to the Minister and/or the CWG in Canberra.

A Cybersafety and YAG Summit was held on 8 June 2010 where members, parents and teachers provided their views on a range of government cybersafety programs and initiatives including the above mentioned Cybersafety Help Button and Teachers and Parents Advisory Group, the *budd:e* cybersecurity educational modules and the *ThinkuKnow* program administered by the Australian Federal Police. The advice received is being used to further develop these projects.

The CWG considers that the YAG will be critical to further development of cybersafety policy and acknowledges that it will be essential that all stakeholders be responsive in considering the Group's advice. The CWG will track the advice of the YAG closely and ensure that this is taken into account and acted upon, as appropriate.

#### **4.6 Ensuring that the CWG's deliberations take account of new technologies**

The CWG considered a range of new technologies to mitigate cybersafety risks.

##### *Technical measures employed by CWG members*

MySpace has more than 110 million monthly active users around the globe, 1.5 million of which are in Australia. MySpace approaches the safety, security, and privacy of its users with a holistic strategy, one component of which is technology. For example, to combat a situation where an underage minor lies about his or her age, MySpace employs a strengthened search algorithm, utilizing terms commonly used by underage users, to find and delete underage profiles. Profiles are scanned for such terms, and the database of search terms is updated to reflect changes in user behaviour and terminology.

Images and videos reviewed by MySpace that are deemed in violation of MySpace's Terms of Use agreement (such as pornography or copyrighted material) are removed. MySpace also employs hashing technology to ensure that image files identified and deleted as pornography cannot be uploaded again. Child exploitation material, when located, is also hashed and reported to the proper regional authorities.

Through a combination of technology, education, and partnerships MySpace strives to create the safest environment possible for all of its users.

Google has developed its own [SafeSearch filter](#), which uses advanced technology to block pornographic and explicit content from search results. Users can customise their SafeSearch settings by clicking on the “Preferences” link to the right of the search box on Google.com. Google, through acquisition, is also the owner of the video-sharing website, YouTube.

YouTube is a user-generated video sharing platform around which communities form, have discussion and interact. Google’s efforts to maintain the safety and integrity of YouTube comprise four primary elements:

1. Clear policies regarding what is and is not acceptable
2. Robust enforcement mechanisms for these policies
3. Innovative product features that enable safer behaviour, and
4. Education to increase user awareness of how to stay safe.

Further detail on these components can be found at [Attachment F](#).

Microsoft assists home users with free downloadable security tools, and assists law enforcement authorities by, among other things, providing training for officers. In Australia, Microsoft collaborated with the AFP and Ninemsn to launch an Australian version of the successful UK *ThinkuKnow* cybersafety site.

Microsoft has also outlined to the CWG a proposal for an Australian pilot of its digital age verification technology. The CWG digital age verification sub-committee was established to consider Microsoft’s proposal for such a pilot, using schools to verify the ages of the children that would be involved. The sub-committee intends to develop the proposal for the CWG’s consideration, in the first instance, with Microsoft and other industry members of the CWG providing a lead in the sub-committee. The sub-committee met on 9 October, 9 February 2009 and 8 June 2010.

Microsoft also recommends numerous steps that can be taken to parents to foster a safe online experience including using a form of parental control software.

For example, Windows 7 Parental Controls are designed to put parents' minds at ease and give them confidence in their ability to manage what their children can do on the computer. Parental Controls in Windows 7 help parents determine which games their children can play, which programs they can use, and which websites they can visit—and when. Parents can restrict computer use to specific times and trust that Windows 7 will enforce those restrictions, even when they're away from home. These include:

- **Web Restrictions** – Using an online service, a parent can restrict what types of web sites their child can visit, either by category or specific URL to determine what sites are allowed and which are not. These restrictions will work automatically with any web browser.
- **Game Restrictions** – Partnering with Computer Game rating systems from around the world, Windows 7 allows a parent to restrict the types of computer games that their child can play.
- **Application Restrictions** – If a parent chooses, they can apply limits so their child can only run the applications that the parent has approved.

- Time Limits - Parents can decide when children are allowed, or not allowed, to use the computer by choosing the specific times and days to block. The child then receives a 15-minute and a 1-minute notification that their time is about to expire, and if their time ends before they log off the computer, Windows 7 suspends their session and displays the logon screen so another user can use the computer. The child's session stays active in the background, however, so the next time they log on, they can pick up where they left off without losing any of their work.

Telstra has developed the BigPond Home Security Suite—a comprehensive security software package that provides protection from inappropriate content, spam, viruses, and phishing attacks. A subscription includes automatic updates and a 24 hour helpdesk service. The parental controls contained in the BigPond Security Suite allow parents to:

- set time limits on their children's internet usage
- monitor the sites their children visit and provide parent's with reports of their browsing history
- block known problem sites and filter websites for inappropriate language, images and topics—all depending on each child's age group, and
- tailor protection for their family and their PC using pre-set filters and flexible controls.

Telstra is continuing to evaluate technologies which aim to enable the blocking of a defined blacklist of URLs and are sharing the results of their evaluations with the Government.

The CWG will also consider the cybersafety websites of other countries, to see what might be usefully applied to Australia, including different methods for users to report abuse.

#### ISP filtering

##### *International initiatives*

Internet Service Provider (ISP) filtering has been voluntarily adopted by ISPs in a number of countries, including the UK, Canada, Norway, Sweden, Finland and Denmark. In most instances this involves the filtering of blacklists of child sexual abuse material. The New Zealand Department of Internal Affairs has introduced a centralised filtering system, the Digital Child Exploitation Filtering System, which New Zealand ISPs can use to block websites that host child sexual abuse images.

The CWG will monitor other technical initiatives taken overseas for their relevance for Australia, including the above initiative taken by Google in Germany to block certain black-listed sites from search results.

##### *Australia*

The CWG notes that a small number of ISPs in Australia have implemented ISP filtering as part of their business. Webshield, for example, provides customised content filtering for users with filtering available in relation to: over 90 content categories; 'blacklists' and 'whitelists'; word search and key word filtering; peer to peer and chat protocol management; and prevention of proxy bypass.

Other small ISPs who have recently entered the market also have implemented ISP level filtering services as part of their business model.

The CWG has been kept informed of the ISP filtering live pilot conducted by the Department. The live pilot provided information on filters installed in ISP networks. In particular, the CWG understands the pilot tested:

- impact on network speed
- accuracy of filters (over/ under blocking)
- circumvention
- ease of use from an end-user's perspective
- costs
- scalability, and
- effectiveness of additional functionalities.

The pilot examined the filtering solutions proposed by applicants, ranging from simple blocking of the ACMA blacklist to potentially more sophisticated solutions, providing families with options to block a wider range of content if they wish. A report on findings from the pilot was released in December 2009.

Recently, Telstra, Optus and Primus have agreed to voluntarily filter a list of child abuse URLs.

These three ISPs account for around 70 per cent of the broadband customer market and their actions may encourage other ISPs to follow suit.

This voluntary initiative will be supported by ACMA, who will provide ISPs with a list of URLs relating to child abuse material for filtering. This is based on community complaints and incorporates similar lists from respected international child sexual abuse agencies.

More information about ISP filtering is available on the DBCDE web site.

#### **4.7 Review mechanisms**

The CWG notes the addition to the Committee's Terms of Reference to include consideration of the merits of establishing an Online Ombudsman to investigate, advocate and act on cybersafety issues. Many websites operate on a global basis and often only have a minimal presence in Australia. The CWG considers there would be significant limitations as to what an Australian Ombudsman can legally oversight and report on. In addition, without jurisdiction over sites hosted outside Australia, the scheme would rely on voluntary compliance without any guarantees that this would occur which would in turn undermine the effectiveness of an Online Ombudsman.

In Australia there are already several mechanisms for dealing with online complaints established by the ACMA, the AFP, ACCC, and the Privacy Commissioner. Establishing yet another mechanism may exacerbate existing confusion in the minds of the public as to where to direct complaints and potentially add time and complexity to complaint resolution without necessarily improving outcomes for consumers. It would be necessary to clarify the existing roles and look at ways of removing duplication if an Online Ombudsman were introduced.



The CWG considers that there are other ways to safeguard the interests of consumers, as has occurred overseas. For example, the European Union's Safer Social Networking Principles, which most major social networking sites have signed up to, provide an alternative and means of regulating the sector. Approaches such as this need to be explored further as they are more likely to include a larger proportion of the internet community.

## 5. Operation of the CWG

The CWG has worked well, with good attendance and discussion of the issues at hand.

CWG membership is for a period of 12 months, at which time members are given the opportunity to renew or resign their membership. Refer to Attachment A.

## 6. References

Australian Communications and Media Authority (ACMA), *Media & Communications in Australian Families, Report of the Media & Society Research Project* (2007).

Australian Communications and Media Authority (ACMA), *Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety: Second Annual Report to the Minister for Broadband, Communications and the Digital Economy* (2008).

Australian Communications and Media Authority (ACMA), *Australia in the Digital Economy: Trust and Confidence* (2009).

Australian Communications and Media Authority (ACMA), *Click and Connect: Young Australians' use of online social media* (2009).

Australian Institute of Criminology (AIC), *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences* (2009).

Berrier, T *Sixth-, seventh-, and eighth-grade students' experiences with the Internet and their Internet safety knowledge*, Dissertation presented to the East Tennessee State University (2007)

Boyd, D 'Why Youth ♥ Social Network Sites: The Role of Networked Publics in Teenage Social Life', in Buckingham, D (ed), *Youth, Identity, and Digital Media*, The John D and Catherine T MacArthur Foundation Series on Digital Media and Learning, Cambridge MA, The MIT Press, pp 119-142 (2008).

Bryant, C *Adolescence, pornography and harm*, Trends and Issues in Crime and Criminal Justice, Australian Institute of Criminology, No. 368, February 2009.

Byron, T, *Safer children in a Digital World—The Report of the Byron Review* (2008).

Cross, D et al, *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre, Edith Cowan University, 2009.

European Commission (EC) (by Optem), *Safer Internet for Children, Qualitative Study in 29 European Countries Summary Report* (2007).

European Commission (EC), *Towards a Safer Use of the Internet for children in the EU—a parents' perspective*, Flash Eurobarometer survey, 2008.

Hanewald, R, Confronting the Pedagogical Challenge of Cyber Safety, *Australian Journal of Teacher Education*, Vol 33, 3, June 2008.

Internet Safety Technical Task Force (US) *Enhancing Child Safety and Online Technologies* (Final Report) (2008).

Khan MK, *Emotional And Behavioural Effects, Including Addictive Potential Of Video Games*, Report Of The Council On Science And Public Health (US), CSAPH Report 12-A-07 (2007).

Livingstone, S and Bober, M, *UK Children Go Online*, Economic & Social Research Council (2005).

Livingstone, S and Helsper, EJ, Taking risks when communicating on the Internet: the role of offline social-psychological factors in young people's vulnerability to online risks, *Information, Communication & Society*, Vol 10(5) (2007), pp 619-644.

Livingstone, S, and Haddon, L, (2009) *EU Kids Online: Final Report*, LSE, London: EU Kids Online. (EC Safer Internet Plus Programme Deliverable D6.5).

Organisation for Economic Cooperation and Development (OECD), Ministerial Declaration *Shaping Policies for the Future of the Internet Economy*, June 2008.

Spears, B, Johnson, B, Slee, P, and Owens L, *Behind the Scenes: Insights into the Human Dimension of Covert Bullying*, University of South Australia and Flinders University, 2009.

Tynes, BM, 'Internet Safety Gone Wild? Sacrificing the Education and Psychosocial Benefits of Online Social Environments' *Journal of Adolescent Research*, Vol. 22(6), 575-584 (2007).

Withers, K with Sheldon, R *Behind the Screen, the hidden life of youth online* Research paper by the Institute for Public Policy Research (UK) (2008)

Wolak, J; Mitchell, K; Finkelhor, D 'Unwanted and Wanted Exposure to Online Pornography in a National Sample of youth Internet Users, *Pediatrics*, 119, pp 247-257 (2007)

**Consultative Working Group on Cyber-safety:  
Membership 2010-2011**

<b>Member</b>	<b>Title</b>	<b>Organisation</b>
Mr Abul Rizvi (Chair)	Deputy Secretary	Department of Broadband, Communications and the Digital Economy
Dr Judith Slocombe	Chief Executive Officer	Alannah and Madeline Foundation
Ms Hetty Johnston	Executive Director	Bravehearts Inc
Ms Bernadette McMenamin AO	Chief Executive Officer	ChildWise
Mrs Sue Hutley	Executive Director	Australian Library and Information Association
Mr Chris Althaus	Chief Executive Officer	Australian Mobile Telecommunications Association
Mr Peter Coroneos	Chief Executive Officer	Internet Industry Association
Mr Darren Kane	Director Corporate Security & Investigations	Telstra Corporate Limited
Mr Anthony Pillion	Manager	Webshield
Mr Nick Abrahams	Partner	Norton Rose
Ms Ishtar Vij	Public Policy and Government Affairs	Google Australia and New Zealand
Mr Jeff Bullwinkel	General Counsel Head of Legal and Corporate Affairs	Microsoft Pty Ltd
Mr Matthew Strathdee	Director of Business & Legal Affairs Asia Pacific	Fox Interactive Media
Ms Samantha Yorke	Acting General Counsel	Yahoo! Group Australia & New Zealand
Mr Ron Curry	Chief Executive Officer	Interactive Entertainment Association of Australia
Mr Mozelle Thompson	Adviser	Facebook
Ms Nerida O'Loughlin	General Manager	Australian Communications and Media Authority

<b>Member</b>	<b>Title</b>	<b>Organisation</b>
Assistant Commissioner Neil Gaughan	Assistant Commissioner	Australian Federal Police
Dr Gabrielle Phillips	Branch Manager	Department of Education, Employment and Workplace Relations
Ms Sarah Chidgey	Assistant Secretary	Attorney-General's Department
Ms Michelle Weston	Section Manager	Department of Families, Housing, Community Services and Indigenous Affairs

## **CONSULTATIVE WORKING GROUP ON CYBER-SAFETY**

### **TERMS OF REFERENCE**

As part of the Rudd Labor Government's Cyber-safety plan, the Consultative Working Group will:

- consider those aspects of cyber-safety faced by Australian children;
- provide information to Government on measures required to operate and maintain world's best practice safeguards for Australian children engaging in the digital economy; and
- advise the Government on priorities for action by government and industry.

The Consultative Working Group's considerations will include:

1. 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);
2. the nature, prevalence and implications of cyber-safety threats, such as:
  - abuse of children online (cyber-bullying, cyber-stalking and sexual grooming);
  - exposure to illegal and inappropriate content;
  - promotion of inappropriate social and health behaviours (technology addiction, anorexia, drug usage, underage drinking and smoking);
  - identity theft; and
  - breaches of privacy.
3. Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) and their effectiveness;
4. opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cyber-safety issues;
5. information required to realise the potential for achieving and continuing world's best practice safeguards; and
6. ensuring that their deliberations take account of new technologies and the changing nature of the cyber-safety environment and continue to remain relevant.

The Consultative Working Group will consider the reports of its Sub-Committees and a Youth Advisory Group on cyber-safety issues for children and how to deliver effective solutions.

The Committee is also to inquire into and report on such other matters relating to cyber-safety that may be referred to it by the Minister for Broadband, Communications and the Digital Economy.

**EXAMPLES OF AUSTRALIAN CYBER-SAFETY AND YOUTH OUTREACH INITIATIVES, AND UNPUBLISHED AUSTRALIAN RESEARCH**

**Cyber-safety Initiatives**

- The Australian Government's Cyber-safety Plan which includes:
  - the formation of the Youth Advisory Group and its associated website, *y@g Online*; and
  - the work by the Australian Communications and Media Authority to develop a cyber-safety schools 'gateway' which will support a whole school approach to cyber-safety.
- The Australian Federal Police's *Today's Youth Forum* which provides an interactive site through MySpace and focuses on cyber-safety issues.
- The *SuperClubsPlus Australia* social networking site funded by the Telstra Foundation.
- The Alannah and Madeline Foundation's *CyberSmart Campaign*: a proposed system to accredit primary and secondary schools that have policies in place that encourage the use of technologies such as the internet and mobile phones in safe and responsible ways.

**Outreach, which may include cyber-safety topics**

- The *Cybersmart Kids Online* site, hosted by ACMA.
- The *ThinkUKnow* site, hosted by the AFP and Microsoft.
- The *Australian Youth Forum*, announced by the Minister for Youth Affairs, the Hon Kate Ellis MP, which includes an interactive site.
- The *Bullying. No way!* site: has an interactive component and a section on cyber-bullying—created by Australia's educational communities (State, Territory and Commonwealth government education departments, and Catholic and independent education sectors).
- The *Kids Help Line*, which provides free, confidential and anonymous, telephone and online counseling services for young people aged between 5 and 25.
- The *Smart Online Safe Offline* program of the National Association for Prevention of Child Abuse and Neglect, designed to teach children aged 9 to 14 years to stay safe online as well as providing support for parents, teachers and the community.
- Centacare Sandhurst's *Loddon Mallee Cyber Safety program*, a Bendigo-based not-for-profit organisation with a rural and provincial focus.
- Edith Cowan University in Western Australia's *Child Health Promotion Research Centre*, which is developing a parent education program that will test educational strategies designed to help parents increase their child's cyber safety.
- The New South Wales Youth Advisory Council (YAC) set up to advise the NSW Government on issues of concern to young people (aged 12-25) in NSW, Government policies relating to young people, and youth-related programs.
- The *Queensland Youth Council*, which provides a forum for the exchange of information and views between young people and the Queensland Government.

- The *Student Youth Network* in Melbourne, which will get a small team of its young volunteer reporters to research and discuss cyber safety on its radio and television stations and online.
- The Child Health Promotion Research Centre's (Edith Cowan University) *Parent Education Program*, providing parents with support and advice on how to deal with cyber safety.
- Australian Institute of Criminology's publication, *Cyber-bullying issues for policy makers*, No. 59, 2007.
- Mental Health Association NSW Inc's Fact Sheet, *Cyber Bullying*, 2008.

**Unpublished Cyber-safety Related Research and Inquiries**

- Two research projects to be commissioned by the Australian Government under the Cyber-safety Plan: a review and analysis of existing cyber-safety research and a repeatable survey.
- The Child Health Promotion Research Centre's (Professor Donna Cross, et al, Edith Cowan University) *Covert Bullying – Its Nature and Prevalence in Australian Schools*, funded by the Department of Education, Employment and Workplace Relations.
- The Child Health Promotion Research Centre's (Professor Donna Cross, et al, Edith Cowan University), *How Cyber Technology is Affecting Relational Aggression and Teenage Health*, funded by Healthway.
- Queensland University of Technology (Dr Marilyn Campbell et al) *'Cyber bullying: an evidence-based approach to the application and reform of law, policy and practice in schools'* funded by the Australian Research Council Linkage.
- The Child Health Promotion Research Centre's (Edith Cowan University) *Western Australian Cyber Friendly Student Summit*, part of a \$400,000 study into cyber bullying prevention funded by the Western Australian Government.

## **JOINT STATEMENT ON KEY PRINCIPLES OF SOCIAL NETWORKING SITES SAFETY**

Because improving internet safety for children is a critical public policy objective, Facebook and the Attorneys General agree to the following principles:

**PRINCIPLE:** Providing children with a safer social networking experience is a primary objective for operators of social networking sites.

### **I. ONLINE SAFETY TOOLS**

**PRINCIPLE:** Technology and other tools that empower parents, educators and children are a necessary element of a safer online experience for children.

**PRINCIPLE:** Online safety tools, including online identity authentication technologies, are important and must be robust and effective in creating a safer online experience, and must meet the particular needs of individual Web sites.

- The social networking site will participate, with support of the Attorneys General, in an industry-wide Internet Safety Technical Task Force (“Task Force”) devoted to finding and developing such online safety tools with a focus on finding and developing online identity authentication tools. This Task Force will include Internet businesses, identity authentication experts, non-profit organizations, and technology companies.
- The Task Force will establish specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions
- The social networking site will provide adequate resources to ensure that all reasonable efforts are made to explore and develop identity authentication technologies.
- The social networking site will designate a senior executive to work with the Task Force.
- The Task Force will provide the Executive Committee of the Attorneys General Social Networking Working Group (“Executive Committee”) with quarterly reports of its efforts and presentation of a formal report by the end of 2008. The Executive Committee will have continuing access to the Task Force and the designated senior executive of the social networking site.



## II. DESIGN AND FUNCTIONALITY CHANGES

**PRINCIPLE:** Development of effective Web site design and functionality improvements to protect children from inappropriate adult contacts and content must be an ongoing effort.

- The social networking site and the Attorneys General share the goal of designing and implementing technologies and features that will make the site safer for its users, particularly minors. More specifically, their shared goals include designing and implementing technologies and features that will (1) prevent underage users from accessing the site; (2) protect minors from inappropriate contact; (3) protect minors from inappropriate content; and (4) provide safety tools for all social networking site users. These design and functionality changes are set forth in Appendix A.
- The social networking site and the Attorneys General will meet on a regular basis to discuss in good faith design and functionality improvements relevant to protecting minors using the Web site.

## III. EDUCATION AND TOOLS FOR PARENTS, EDUCATORS, AND CHILDREN

**PRINCIPLE:** Educating parents, educators and children about safe and responsible social networking site use is also a necessary part of a safe Internet experience for children.

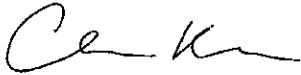
- The social networking site will continue to dedicate meaningful resources to convey information to help parents and educators protect children and help younger users enjoy a safer experience. These efforts will include the site's intent to engage in public service announcements, promote free parental monitoring software, and explore the establishment of a children's email registry.
- The social networking site shall use its best efforts to acknowledge consumer reports or complaints via its abuse reporting mechanisms within 24 hours of receiving such report or complaint. Within 72 hours of receiving a complaint or report from a consumer regarding inappropriate content or activity on the site, the social networking site will report to the consumer the steps it has taken to address the complaint.
- For a two (2) year period the social networking site shall retain an Independent Examiner, at the site's expense, who shall be approved by the Executive Committee. The Independent Examiner shall evaluate and examine the social networking site's handling of these consumer complaints and shall prepare bi-annual reports to the Executive Committee concerning the site's consumer complaints handling and response procedures, as provided above.

#### IV. LAW ENFORCEMENT COOPERATION

**PRINCIPLE:** Social networking site operators and law enforcement officials must work together to deter and prosecute criminals misusing the Internet.

- The social networking site and the Attorneys General will work together to support initiatives that will enhance the ability of law enforcement officials to investigate and prosecute Internet crimes.
- The social networking site and the Attorneys General will continue to work together to make sure that law enforcement officials can act quickly to investigate and prosecute criminal conduct identified on its site.
- The social networking site will establish a 24-hour hotline to respond to law enforcement inquiries. In addition, the social networking site will assign a liaison to address complaints about its site received from the Attorneys General. The social networking site will provide a report on the status of its response to any such complaint within 72 hours of receipt by the liaison.

Agreed to and accepted on May 8, 2008:



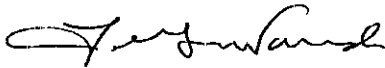
Chris Kelly  
Chief Privacy Officer, Facebook



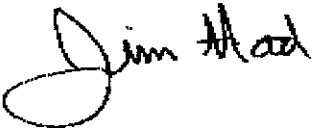
Richard Blumenthal  
Attorney General of Connecticut



Peter Nickles  
Interim Attorney General of D.C.



Lawrence Wasden  
Attorney General of Idaho



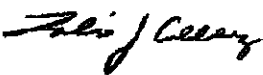
Jim Hood  
Attorney General of Mississippi



Marc Dann  
Attorney General of Ohio



Robert McDonnell  
Attorney General of Virginia



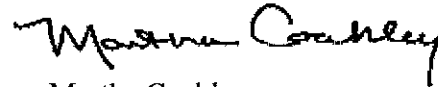
Talis J. Colberg  
Attorney General of Alaska



Roy Cooper  
Attorney General of North Carolina



Thurbert E. Baker  
Attorney General of Georgia



Martha Coakley  
Attorney General of Massachusetts



Kelly Ayotte  
Attorney General of New Hampshire



Tom Corbett  
Attorney General of Pennsylvania



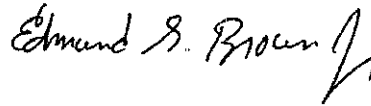
Troy King  
Attorney General of Alabama



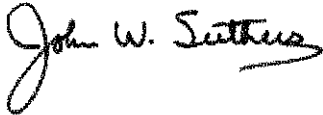
Terry Goddard  
Attorney General of Arizona



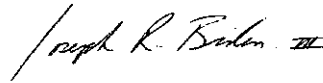
Dustin McDaniel  
Attorney General of Arkansas



Edmund G. Brown, Jr.  
Attorney General of California



John W. Suthers  
Attorney General of Colorado



Joseph R. Biden, III  
Attorney General of Delaware



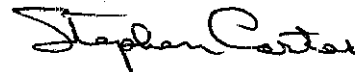
Bill McCollum  
Attorney General of Florida



Mark J. Bennett  
Attorney General of Hawaii



Lisa Madigan  
Attorney General of Illinois



Stephen Carter  
Attorney General of Indiana



Tom Miller  
Attorney General of Iowa



Stephen N. Six  
Attorney General of Kansas



Jack Conway  
Attorney General of Kentucky



James D. "Buddy" Caldwell  
Attorney General of Louisiana



Steven Rowe  
Attorney General of Maine



Douglas Gansler  
Attorney General of Maryland



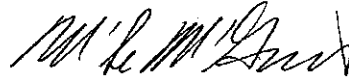
Michael A. Cox  
Attorney General of Michigan



Lori Swanson  
Attorney General of Minnesota



Jeremiah W. "Jay" Nixon  
Attorney General of Missouri



Mike McGrath  
Attorney General of Montana




Jon Bruning  
Attorney General of Nebraska



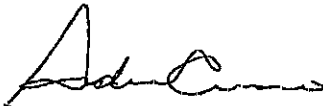
Catherine Cortez Masto  
Attorney General of Nevada



Anne Milgram  
Attorney General of New Jersey



Gary King  
Attorney General of New Mexico



Andrew M. Cuomo  
Attorney General of New York



Wayne Stenehjem  
Attorney General of North Dakota



W.A. Drew Edmondson  
Attorney General of Oklahoma



Hardy Myers  
Attorney General of Oregon



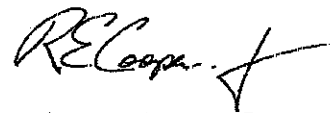
Patrick C. Lynch  
Attorney General of Rhode Island



Henry McMaster  
Attorney General of South Carolina



Lawrence E. Long  
Attorney General of South Dakota



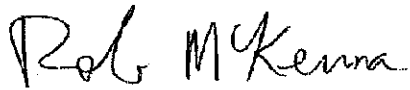
Robert E. Cooper, Jr.  
Attorney General of Tennessee



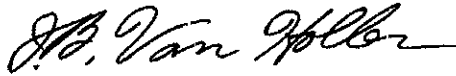
Mark L. Shurtleff  
Attorney General of Utah



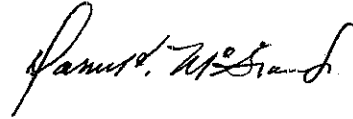
William Sorrell  
Attorney General of Vermont



Rob McKenna  
Attorney General of Washington



J.B. Van Hollen  
Attorney General of Wisconsin



Darrell V. McGraw, Jr.  
Attorney General of West Virginia



Bruce A. Salzburg  
Attorney General of Wyoming

## **APPENDIX A: DESIGN AND FUNCTIONALITY FEATURES**

### **Preventing Underage Users**

1. The site will enforce “age locking” for existing and new profiles such that members shall be required to have their profile reviewed by a customer service representative before any user-initiated age change after initial registration if they are under 18, or if they seek to change their age to indicate they are under 18. The site recognizes a user may mistakenly enter the incorrect age at the time of registration, takes seriously any request to change a user’s age, and will carefully scrutinize any attempt on the part of a user to do so. This will include a thorough review of the profile, including the user’s friends and whether the user is affiliated with a high school network. Requests to change age for users will be logged, and the site will grant only a single request to change age above or below the 18 year old threshold.

### **Protecting Younger Users from Inappropriate Contact**

The site uses and will continue to use technological tools that identify potentially inappropriate approaches to minors. These tools take into account many actions that could be taken by a user on the site, including some described below, to determine whether an individual user’s actions merit attention and/or action from the site. The site then takes appropriate action as necessary to limit or forbid site access to users based on their inappropriate activity.

1. The site shall by default use real world social factors, such as a shared network, to restrict access to a minor’s profile.
2. Users under 18 can block all users over 18 from contacting them or viewing their profile.
3. Users over 18 will be limited to search in the school section only for high school students graduating in the current or upcoming year.
4. Users over 18 may restrict access to profile information to users under 18, and users under 18 will have default settings that limit access to personal information to non-friend users over 18.
5. Limit search engine ability to crawl all private profiles.
6. The site shall use reasonable means to determine whether or not a user is in fact a member of a school network with which they attempt to affiliate (e.g., verification by network members, ongoing technological assessment of user interactions) and shall provide an easy means to report members who do not belong in a particular network. As more robust tools for school network or other identity/affinity

analysis become available (e.g., school-issued email), site will implement those advanced tools.

7. The site shall set restrictions on the display of offline contact information (e.g. telephone number, address) in profiles and rapidly remove postings of such information in public forums upon report.
8. The site will not allow unregistered visitors to view search results related to age-restricted areas of the site, including groups and forums geared toward sexual activity and mature content.
9. All posting of images and private messages on the site shall be linked to a user account.
10. No over-18 user should be able to perform an age-based search for anyone under 18. In addition, Facebook shall assess search/browse functions for potential misuse and regularly update the Attorneys General of such efforts.
11. Search terms that are commonly used to locate minors (searching specific keywords, reviewing groups and forums, and browsing certain age ranges) shall be identified and monitored.
12. Profiles of registered sex offenders identified using appropriate technology are reviewed and, once confirmed, are removed from the site. The associated data are preserved for law enforcement.

### **Protecting Younger Users from Inappropriate Content**

The site uses and will continue to use technological tools that identify posting of potentially inappropriate content on the site. These tools take into account many actions that could be taken by a user on the site, including some described below, to determine whether an individual user's actions merit attention and/or action from the site. The site then takes appropriate action as necessary to limit or forbid site access to users based on their inappropriate activity.

1. Policy for hosted images shall employ technology to rapidly block and remove image uploads that violate the Terms of Use and block accounts of those who attempt to upload such images.
2. Ensure report functionality that allows users to select from specific categories of abuse. These categories may include fake profile, underage user or non-network member, inappropriate contact, spam/scam/phishing, nudity or pornography, suicide threat, harassment, violence, attacks individual or group, etc.
3. The site will regularly review models for abuse reporting and will perform a test using the New Jersey Attorney General's common abuse reporting icon. If the



site, in its sole discretion, determines that the New Jersey common abuse reporting icon is workable and will improve user safety, and the New Jersey Attorney General consents to its use, the site may use the common icon in place of or in conjunction with the current report abuse links.

4. Abuse reporting mechanisms shall be relevant and designed to be easily available to users.
5. Tobacco and alcohol advertisements, if accepted, are targeted only to those of legal age to purchase the products.
6. Events shall provide organizer with tools to designate appropriate minimum age for attendance at any event, and site shall not display event to those under the designated age. False designation of minimum appropriate age for an event shall be a violation of the site terms of service and site shall take action to warn or remove any user falsely indicating age-appropriateness for an event upon report or discovery.
7. The site will notify users whose profiles are deleted for Terms of Service violations.
8. Groups or forums reported for incest, pedophilia, cyberbullying, or other violations of the Terms of Use are removed, with violators removed from site.
9. Facebook will (1) further develop its deployment of technology such as textual searching; and (2) provide increased staff, if appropriate, in order to more efficiently and effectively review and categorize content in "Groups." Facebook will regularly update the Attorneys General concerning its efforts to develop and/or use textual searching and advanced technologies for the detection and removal of inappropriate content.
10. Members determined to be under 18 shall be removed upon report or discovery from groups or pages promoting adult (pornographic) content, tobacco or alcohol without violating the terms of service, along with any posts the under-18 user has made. Such groups determined to be created by under-18 members shall be removed entirely and the user accounts may be deleted for violating the Terms of Service.
11. Users under 18 will not have access to content rated only for over-18s.
12. Groups that are not appropriate for all ages shall carry designations by creators indicating the appropriate age for access to the group.
13. Site shall deny access to groups by users who do not meet the age requirement.

14. User accounts promptly deleted for uploading child pornographic images and/or videos and referred to NCMEC.
15. The site does not tolerate posting of pornography, and shall have a system that warns users determined to have uploaded pornographic images and/or videos. Abuse of this rule shall result in termination of the user account.
16. Maintain a list of adult (pornographic) Web sites on an ongoing basis and sever all active links to those sites from the site.
17. The site will maintain enforceable privacy and safety guidelines for third party applications available to users through the site.

**Providing Safety Tools For All Members**

1. All users shall have extensive privacy controls to enable them to choose who can see their profile and particular information within it.
2. All users should have reasonable mechanisms to control comments on their profile or “wall”.
3. Users can block another user from contacting them.
4. Users can conceal their “online now” status.
5. Users can control who has access to their images using privacy settings
6. The site includes “Report” links in relevant places throughout the site.
7. Users under 18 can block over-18 users from contacting them or viewing their profiles.
8. All users can allow only those users whom they have added to their friends list to see when they are present on the site and to contact them.
9. “Safety Tips” should be readily available throughout the site and promoted to minors regularly in contextually relevant places.
10. Safety Tips contain resources for Internet Safety, including FTC Tips.
11. Phishing warning shall be contained in Safety Tips.
12. Safety Tips for Parents should provide suggestions on the use of computer-based blocking software

13. Parents are able to remove underage child's profile through an easily available process.
14. Users under 18 must affirmatively consent that they have reviewed the Safety Tips prior to registration. Facebook will further promote Safety Tips as part of the site orientation and regularly include safety messaging where there is a significant risk of an under-18 user revealing personal information to an unknown adult.

**JOINT STATEMENT ON  
KEY PRINCIPLES OF SOCIAL NETWORKING SITES SAFETY**

MySpace and the Attorneys General have discussed social networking sites safety measures with great vigor over several months. MySpace and the Attorneys General agree that social networking sites are a powerful communications tool that provides people with great social benefits. However, like all communication tools, social networking sites can be misused as a means to commit crimes against minors and can allow minors to gain access to content that may be inappropriate for them.

- MySpace and other members of the Task Force will provide adequate resources to ensure that all reasonable efforts are made to explore and develop identity authentication technologies.
- News Corporation will designate a senior executive to work with the Task Force.
- The Task Force will provide the Executive Committee of the Attorneys General Social Networking Working Group (“Executive Committee”) with quarterly reports of its efforts and presentation of a formal report by the end of 2008. The Executive Committee will have continuing access to the Task Force and the designated senior executive of News Corporation.

## **II. DESIGN AND FUNCTIONALITY CHANGES**

**PRINCIPLE:** Development of effective Web site design and functionality improvements to protect children from inappropriate adult contacts and content must be an ongoing effort.

- MySpace and the Attorneys General share the goal of designing and implementing technologies and features that will make MySpace safer for its users, particularly minors. More specifically, their shared goals include designing and implementing technologies and features that will (1) prevent underage users from accessing the site; (2) protect minors from inappropriate contact; (3) protect minors from inappropriate content; and (4) provide safety tools for all MySpace users.
- The Attorneys General acknowledge that MySpace is seeking to address these goals by (1) implementing the design and functionality initiatives described in Appendix A; and (2) working to implement the design and functionality initiatives described in Appendix B.
- MySpace and the Attorneys General will meet on a regular basis to discuss in good faith design and functionality improvements relevant to protecting minors using the Web site.

## **III. EDUCATION AND TOOLS FOR PARENTS, EDUCATORS, AND CHILDREN**

**PRINCIPLE:** Educating parents, educators and children about safe and responsible social networking site use is also a necessary part of a safe Internet experience for children.

- MySpace will continue to dedicate meaningful resources to convey information to help parents and educators protect children and help younger users enjoy a safer experience on MySpace. These efforts will include MySpace's plan to engage in public service announcements, develop free parental monitoring software, and explore the establishment of a children's email registry.
- MySpace shall use its best efforts to acknowledge consumer reports or complaints received via its abuse reporting mechanisms within 24 hours of receiving such report or complaint. Within 72 hours of receiving a complaint or report from a consumer regarding inappropriate content or activity on the site, MySpace will report to the consumer the steps it has taken to address the complaint.
- For a two (2) year period MySpace shall retain an Independent Examiner, at MySpace's expense, who shall be approved by the Executive Committee. The Independent Examiner shall evaluate and examine MySpace's handling of these consumer complaints and shall prepare bi-annual reports to the Executive Committee concerning MySpace's consumer complaint handling and response procedures, as provided above.

#### IV. LAW ENFORCEMENT COOPERATION

**PRINCIPLE:** Social networking site operators and law enforcement officials must work together to deter and prosecute criminals misusing the Internet.

- MySpace and the Attorneys General will work together to support initiatives that will enhance the ability of law enforcement officials to investigate and prosecute Internet crimes.
- MySpace and the Attorneys General will continue to work together to make sure that law enforcement officials can act quickly to investigate and prosecute criminal conduct identified on MySpace.
- MySpace has established a 24-hour hotline to respond to law enforcement inquiries. In addition, News Corporation will assign a liaison to address complaints about MySpace received from the Attorneys General. MySpace will provide a report on the status of its response to any such complaint within 72 hours of receipt by the liaison.

Agreed to and accepted on January 14<sup>th</sup>, 2008:



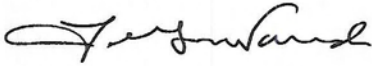
Mike Angus  
EVP, General Counsel, Fox Interactive Media



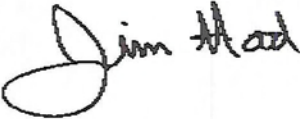
Richard Blumenthal  
Attorney General of Connecticut



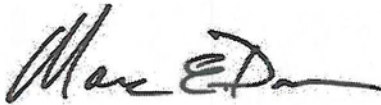
Peter Nickles  
Interim Attorney General of D.C.



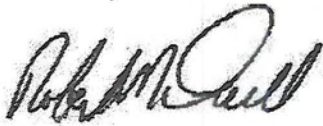
Lawrence Wasden  
Attorney General of Idaho



Jim Hood  
Attorney General of Mississippi



Marc Dann  
Attorney General of Ohio



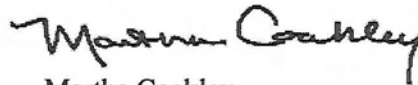
Robert McDonnell  
Attorney General of Virginia



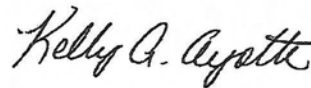
Roy Cooper  
Attorney General of North Carolina



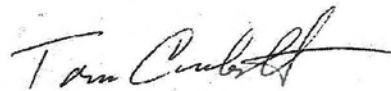
Thurbert E. Baker  
Attorney General of Georgia



Martha Coakley  
Attorney General of Massachusetts



Kelly Ayotte  
Attorney General of New Hampshire



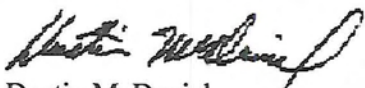
Tom Corbett  
Attorney General of Pennsylvania




Troy King  
Attorney General of Alabama



Talis Colberg  
Attorney General of Alaska



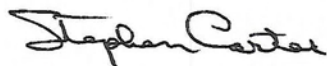
Dustin McDaniel  
Attorney General of Arkansas



Joseph R. Biden III  
Attorney General of Delaware



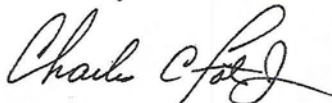
Mark J. Bennett  
Attorney General of Hawaii



Stephen Carter  
Attorney General of Indiana



Paul Morrison  
Attorney General of Kansas



Charles C. Foti, Jr.  
Attorney General of Louisiana



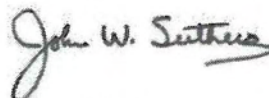
Douglas Gansler  
Attorney General of Maryland



Lori Swanson  
Attorney General of Minnesota



Terry Goddard  
Attorney General of Arizona




John Suthers  
Attorney General of Colorado



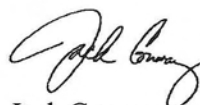
Bill McCollum  
Attorney General of Florida



Lisa Madigan  
Attorney General of Illinois



Tom Miller  
Attorney General of Iowa



Jack Conway  
Attorney General of Kentucky



G. Steven Rowe  
Attorney General of Maine



Michael A. Cox  
Attorney General of Michigan



Jeremiah W. Nixon  
Attorney General of Missouri

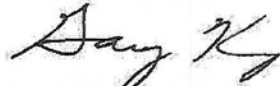




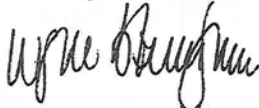
Mike McGrath  
Attorney General of Montana



Catherine Cortez Masto  
Attorney General of Nevada



Gary King  
Attorney General of New Mexico



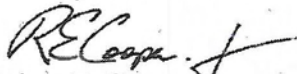
Wayne Stenehjem  
Attorney General of North Dakota



Hardy Myers  
Attorney General of Oregon



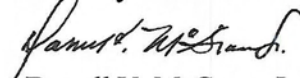
Henry McMaster  
Attorney General of South Carolina



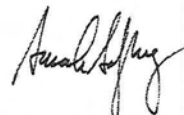
Robert E. Cooper, Jr.  
Attorney General of Tennessee



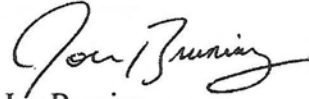
William H. Sorrell  
Attorney General of Vermont



Darrell V. McGraw, Jr.  
Attorney General of West Virginia



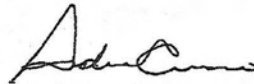
Bruce Salzburg  
Attorney General of Wyoming



Jon Bruning  
Attorney General of Nebraska



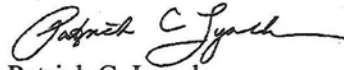
Anne Milgram  
Attorney General of New Jersey



Andrew M. Cuomo  
Attorney General of New York



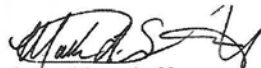
W.A. Drew Edmondson  
Attorney General of Oklahoma



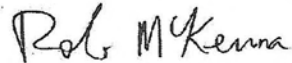
Patrick C. Lynch  
Attorney General of Rhode Island



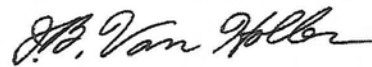
Lawrence E. Long  
Attorney General of South Dakota



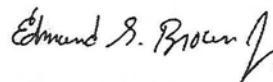
Mark L. Shurtleff  
Attorney General of Utah



Rob McKenna  
Attorney General of Washington



J.B. Van Hollen  
Attorney General of Wisconsin



Edmond G. "Jerry" Brown, Jr.  
Attorney General of California

## **APPENDIX A: DESIGN AND FUNCTIONALITY CHANGES**

### **Preventing Underage Users**

1. Browse function - limit to 68 years and below.
2. MySpace will implement “age locking” for existing profiles such that members will be allowed to change their ages only once above or below the 18 year old threshold. Once changed across this threshold, under 18 members will be locked into the age they provided while 18 and older members will be able to make changes to their age as long as they remain above the 18 threshold. MySpace will implement “age locking” for new profiles such that under 18 members will be locked into the age they provide at sign-up while 18 and older members will be able to make changes to their age as long as they remain above the 18 threshold.

### **Protecting Younger Users from Inappropriate Contact**

1. Users able to restrict friend requests to only those who know their email address or last name.
2. “Friend only” group invite mandatory for 14 and 15 year olds.
3. “Friend only” group invite by default for 16 and 17 years olds.
4. Users under 18 can block all users over 18 from contacting them or viewing their profile.
5. Users over 18 will be limited to search in the school section only for high school students graduating in the current or upcoming year.
6. Users over 18 may designate their profiles as private to users under 18, and users under 18 may designate their profiles as private to users over 18.
7. Limit search engine ability to crawl all private profiles.
8. Users under 18 cannot designate themselves as swingers.
9. Users under 16 are automatically assigned a private profile.
10. Users over 18 cannot browse for users under 18.
11. A user cannot browse for users under 16.
12. Users over 18 cannot add users under 16 as friends unless they know the under 16 user's last name or email address.

13. Personally identifiable information removed upon discovery.
14. Users under 18 cannot browse for swingers.
15. MySpace will not allow unregistered visitors to the site to view any search results related to mature areas of the site, profiles that are private to under 18s, or other groups and forums geared toward sexual activity and mature content.
16. MySpace will change the default for under 18 members to require approval for all profile comments.
17. MySpace will remove the ability for under 18 members to browse the following categories: relationship status, "here for", body type, height, smoke, drink, orientation and income.
18. If users under 16 override their privacy settings, they are still only viewable by other users under 18.
19. When user posts images, they will receive a note including IP address of the computer that uploaded the image.
20. Add sender URL in mail for private messages.
21. Locate underage users (searching specific keywords, reviewing groups and forums, and browsing certain age ranges).
22. Profiles of Registered Sex Offenders identified through Sentinel SAFE technology are reviewed and, once confirmed, are removed from the site. The associated data are preserved for law enforcement.

#### **Protecting Younger Users from Inappropriate Content**

1. Implementation of image policy for hosted images that employs hashing technology to prevent inappropriate image uploads.
2. Expand flag spam/abuse to allow categorization of flagged message.
3. Expand "Report Image" functionality to include a drop down menu that provides members with greater specificity on why they are reporting image. Categories to include Pornography, Cyberbullying, and Unauthorized Use.
4. Under 18s/under 21s cannot access tobacco/alcohol advertisements.
5. MySpace and Attorneys General commit to discuss with Google the need to cease directing age inappropriate linked advertisements to minors.

6. Events may be designated for all ages, for 18 + or for 21+.
7. MySpace will notify users whose profiles are deleted for Terms of Service Violations.
8. Groups reviewed for incest, hate speech or youth sex subjects with violators removed from site.
9. Members determined to be under 18 to be removed from mature Groups.
10. Posts determined to be made to mature Groups by under 18 members to be removed.
11. Any mature Groups determined to be created by under 18 members will be removed entirely and the user accounts may be deleted for violating the Terms of Service.
12. Users under 18 to be denied access to Romance & Relationships Forum and Groups.
13. Users under 18 will not have access to inappropriate parts of Classifieds (dating, casting calls).
14. Members may request to label Groups they create as mature.
15. Flagged Groups are reviewed and categorized by MySpace staff.
16. Members under 18 and non-registered users may not enter or view a Group page that has been designated as mature.
17. MySpace hired a Safety Product Manager.
18. Smoking/Drinking preferences blocked for under 18s/under 21s.
19. User accounts promptly deleted for uploading child pornographic images and/or videos and referred to NCMEC.
20. MySpace does not tolerate pornography on its site, and users determined to have uploaded pornographic images and/or videos flagrantly and/or repeatedly will have their accounts deleted.

#### **Providing Safety Tools For All Members**

1. All users may set profile to private.
2. All users can pre-approve all comments before being posted.

3. Users can block another user from contacting them.
4. Users can conceal their “online now” status.
5. Users can prevent forwarding of their images to other sites.
6. MySpace adds “Report Abuse” button to Email, Video, and Forums.
7. Users over 18 can block under 18 users from contacting them or viewing their profiles.
8. All users can allow only those users whom they have proactively added to their Contact List to see when they are on IM and to contact them.
9. “Safety Tips” Available on every page of MySpace.
10. “Safety Tips” Appear on registration page for anyone under 18.
11. Users under 18 must affirmatively consent that user has reviewed the Safety Tips prior to registration. MySpace will require under 18 members to scroll through the complete Safety Tips upon registration. MySpace will also require under 18 members to review the Safety Tips on an annual basis.
12. Additional warning posted to users under 18 regarding disclosure of personal information upon registration.
13. Safety Tips are posted in the “mail” area of all existing users under 18.
14. Safety Tips contain resources for Internet Safety including FTC Tips.
15. Phishing warning added to Safety Tips.
16. Safety Tips for Parents provides links to free blocking software.
17. Parent able to remove child's profile through the ParentCare Hotline and ParentCare Email.
18. MySpace will have “Tom” become a messenger to deliver Safety Tips to minors on MySpace.
19. All users under 18 receive security warnings before posting content.

## **APPENDIX B: DESIGN AND FUNCTIONALITY INITIATIVES**

MySpace will continue to research and develop online safety tools. Based on recommendations MySpace received from the Attorneys General and online safety advocates, and as a result of the work of its internal safety and engineering teams, MySpace's current plans include the following initiatives:

### **Limiting MySpace Membership to Users 14 and Over**

1. Engage a third-party to build and host a registry of email addresses for children under 18. Parents would register their children if they did not want them to have access to MySpace or any other social networking site that uses the registry. A child whose information matches the registry would not be able to register for MySpace membership.
2. Strengthen the algorithm that identifies underage users.

### **Protecting Minors from Unwanted Contacts by Adults**

1. Change the default setting for 16-17 year olds' profiles from "public" to "private."
2. Create a closed high school section for users under 18. The "private" profile of a 16/17 year old will be viewable only by his/her "friends" and other students from that high school who have been vouched for by another such student. Students attending the same high school will be able to "Browse" for each other.

### **Protecting Minors from Exposure to Inappropriate Content**

1. MySpace will review models for a common abuse reporting icon (including the New Jersey Attorney General's "Report Abuse" icon). If MySpace determines that a common icon is workable and will improve user safety, it may substitute the common icon for the current report abuse icon MySpace places on each member profile.
2. Obtain a list of adult (porn) Web sites on an ongoing basis and sever all links to those sites from MySpace.
3. Demand that adult entertainment industry performers set their profiles to block access to all under 18 users.
4. Remove all under 18 users from profiles of identified adult entertainment industry performers.
5. Retain image review vendor(s) that can effectively and efficiently identify inappropriate content so it can be removed from the site more expeditiously.

6. Investigate the use of an additional image review vendor to provide automated analysis of images to help prioritize images for human review.
7. MySpace will (1) develop and/or use existing technology such as textual searching; and (2) provide increased staffing, if appropriate, in order to more efficiently and effectively review and categorize content in “Groups.” MySpace will update the Attorneys General concerning its efforts to develop and/or use textual searching on a quarterly basis. Upon implementation of textual searching, the Attorneys General will review its efficacy with respect to “Groups” for a period of 18 months.

# **Safer Social Networking Principles for the EU**

10 February 2009



# Table of Contents

- I. About these Principles
- II. Background:
  - a. Understanding potential risk on Social Networking Services
  - b. Safer Social Networking, a multi-stakeholder collaboration
- III. Safer Social Networking Principles
- IV. Evaluating the Safer Social Networking Principles
- V. Annex I – Explanatory note on how these Principles may apply to applications

## I. About these Principles

The providers of Social Networking Services (SNS) listed at the end of this document share a common goal to maximise the benefits of the internet while managing the potential risks to children and young people. In order to protect children and young people<sup>1</sup>, individual companies have developed and continue to evolve safety strategies. In addition, many providers have been heavily involved in multi-stakeholder and cross industry dialogues within the EU aimed at establishing and sharing good practice. These include the *UK Home Office Task Force on Child Protection on the Internet*<sup>2</sup>, the *Human Rights Guidelines for Internet Service Providers*<sup>3</sup> developed by the Council of Europe in co-operation with the European Internet Service Providers Association (EuroISPA) and educational projects such as *Teach Today*<sup>4</sup>. Similar activity is also underway in countries outside the EU<sup>5</sup>.

These Principles have been developed by SNS providers in consultation with the European Commission, as part of its *Safer Internet Plus Programme*, and a number of NGOs, to provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services. SNS providers often operate in multiple territories across Europe and the rest of the world and welcome the opportunity to establish pan-EU principles in this area.

The document outlines the principles by which SNS providers should be guided as they seek to help minimise potential harm to children and young people, and recommends a range of good practice approaches which can help achieve those principles. The guidance is not intended as a 'one size fits all' solution. It is recognized that the communications and internet industry is very diverse and ranges from large global providers to smaller locally run services. SNSs vary greatly in terms of the type of service, the platforms on which they can be consumed, their user demographics, the markets in which they operate and the jurisdictions in which they are based. All of these factors affect the levels and types of risks that are attendant to those services and the strategies that may be appropriate and reasonable to address such risks.

Accordingly, in determining their own safety strategies, providers supporting these principles take into account the particular nature of their services in order to apply the relevant recommendations of these Principles. Therefore, while providers will support all seven Principles, it is for each provider to judge where and how far to apply the document's specific recommendations. These Principles are aspirational and not prescriptive or legally binding, but are offered to service providers with a strong recommendation for their use.

---

<sup>1</sup> For the purposes of this document, the term "children and young people" refers to legal minors. Depending on the jurisdiction in which the service is offered and the applicable law, this refers to users under 18 years old or under 16 years old.

<sup>2</sup> <http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary>. The Home Office Task Force's good practice has now been integrated in to the work of the UK Council for Child Internet Safety.

<sup>3</sup> [http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf\(2008\)009\\_en.pdf](http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf)

<sup>4</sup> [www.teachtoday.eu](http://www.teachtoday.eu).

<sup>5</sup> For example, a number of social networking providers worked with the US Internet Safety Technical Task Force to investigate the role technology could play in the protection of children and young people on the internet. See <http://cyber.law.harvard.edu/research/isttf/documents>

These Principles sit alongside ongoing multi-stakeholder dialogues, in the EU and elsewhere, which collectively aim to shape a consistent and complementary framework on which providers can build and develop strategies to protect children and young people. Providers' application of the Principles, the relevance of this document and the good practices it engenders will be evaluated as outlined below, in consultation with the European Commission and other stakeholders.

These Principles are intended to provide guidance to 'Social Networking Services' which are available to children and young people<sup>6</sup>. In the context of these Principles, the term refers to online services that combine the following features:

- A platform that promotes online social interaction between two or more persons for the purposes of friendship, meeting other persons, or information exchange;
- Functionality that lets users create personal profile pages that contain information of their own choosing, such as the name or nickname of the user, photographs placed on the personal page by the user, other personal information about the user, and links to other personal pages on the service of friends or associates of the user that may be accessed by other users or visitors to the service;
- Mechanisms to communicate with other users, such as a message board, electronic mail, or instant messenger; and
- Tools that allow users to search for other users according to the profile information they choose to make available to other users.

Social Networking Services can be accessed using a range of platforms. The capabilities of individual platforms may vary and a provider may not be able to make available the same features on all platforms. Services can also be available as downloadable applications. Where practicable, providers will endeavour to work within the limitations of these platforms and delivery mechanisms to consider these Principles when their services are distributed in this way.

Increasingly, Application Programming Interfaces (APIs) are a feature of SNSs, harnessing the open, distributed and collaborative nature of the internet. APIs allow third party developer companies to create 'applications' and, in some cases, users can add such applications to their SNS profile, providing them with added utility and functionality. Because applications are a new and evolving feature of SNSs and because the nature of the relationship between application developers and the SNS varies from case to case, SNSs can offer differing levels of assurances to their users in terms of these Principles. These levels of assurances will be outlined in a guidance note in Annex 1.

---

<sup>6</sup> Subject to age restrictions defined by the service provider.

## II. Background

### *Understanding potential risks to children and young people on Social Networking Services*

The internet, along with other new technologies, has brought citizens and consumers enormous benefits over the past fifteen years, in terms of communication, information, e-commerce and entertainment. The latest wave of technologies, grouped as 'web 2.0 technologies', which includes SNSs, has triggered further evolution in the way people, especially young people, communicate with friends, access entertainment and engage with communities of interest.

As with many products and services, the misuse of these technologies can present an element of potential risk to children and young people. SNS providers must assess if and how these potential risks apply to their own services. Potential online risks to children and young people fall into four categories:

- 'Illegal content', such as images of child abuse and unlawful hate speech
- 'Age-inappropriate content', such as pornography or sexual content, violence, or other content with adult themes which may be inappropriate for young people.
- 'Contact', which relates to inappropriate contact from adults with a sexual interest in children or by young people who solicit other young people.
- 'Conduct', which relates to how young people behave online. This includes bullying or victimisation (behaviours such as spreading rumours, excluding peers from one's social group, and withdrawing friendship or acceptance) and potentially risky behaviours (which may include for example, divulging personal information, posting sexually provocative photographs, lying about real age or arranging to meet face-to-face with people only ever previously met online).

With the interactivity that web 2.0 technologies enable, it is also important to remember that in addition to being victims young people can also initiate or participate in anti-social or criminal activities.

### *Safer Social Networking: a multi-stakeholder collaboration*

There are a wide range of stakeholders with a role to play in managing potential risks to children and young people, including online service providers, governments, parents, teachers, users and non-governmental organisations. To date, the experience of managing potential risks from the misuse of various aspects of the internet has shown that the most effective approach is for stakeholders to consult and collaborate with other stakeholders, in addition to performing their own roles. These Principles promote this multi-stakeholder collaboration as the most effective way to manage potential risks on SNSs.

SNS providers that allow either children or both young people and adults to subscribe to their service, have a responsibility to ensure that they have assessed their site for potential risks and put in place appropriate measures and tools designed to mitigate those risks. This document is intended to outline the principles that providers should consider in order to fulfil this responsibility.

In order to set the context for these guidelines, it is useful to briefly outline the roles that other stakeholders play in promoting online safety and how SNS providers can work collaboratively with them.

- **Parents, teachers and other carers:** have an important role to play in both educating and fostering an ongoing dialogue with children and young people in their care about safe and responsible online behaviour. Service providers should provide targeted, easily-accessible and up-to-date information and tools to assist them in doing so. Providers should also explore ways to work with educators, governments and other stakeholders to create resources and other educational vehicles.
- **Governments and public bodies:** should provide children and young people with the knowledge and skills to navigate the internet safely. Governments should ensure that e-safety curricula that accurately reflect current internet services and behaviours are delivered in schools. Governments should also ensure that law enforcement agents and those working in the criminal justice system are equipped with the appropriate training, tools and resources necessary to effectively combat criminal activity conducted online. Governments should work together to ensure that the frameworks for cross-border coordination are effective and efficient<sup>7</sup>.

It is important that all stakeholders, including governments and public bodies, understand new challenges and opportunities as they emerge from the rapidly evolving online space. Service providers can assist governments in maintaining this understanding, and should explore ways to work with governments.

- **Police and other law enforcement bodies:** should ensure that officers have appropriate and relevant training and resources for investigating and prosecuting the illegal use of online services. SNS providers and law enforcement bodies should work collaboratively to share their knowledge of social networking and to support investigations in line with applicable laws.
- **Civil society:** as a whole, and through bodies such as child protection agencies, youth organisations and, counselling services, should collaborate with SNS providers and governments through consultation, dialogue or working groups that address their mutual target groups and challenges online. Increasingly, social networking platforms are being harnessed by mental health, social care and support organisations to raise awareness, educate and to deliver counselling and support to young people online, a development which potentially has many positive outcomes<sup>8</sup>. However, it is important that support

---

<sup>7</sup> For example, Mutual Legal Assistance Treaties (MLATs), which exist between countries and allow for information and other assistance from private and public sources to be shared across borders for the purposes of official investigations and prosecutions.

<sup>8</sup> Providers will pay due regard to good practice recommendations for support service provision within SNS environments being developed in other forums such as [www.technologyforwellbeing.ie](http://www.technologyforwellbeing.ie)

organisations conduct a thorough review of a range of issues including how best to uphold essential ethical and professional practices concerning client welfare, confidentiality, competence, responsibility, and integrity when they are considering delivering services from within a social networking environment.

- **Users themselves:** adults, young people and children should at all times respect a service's terms of use and/or community guidelines. They should also make good use of the education, tools, settings and reporting mechanisms designed to encourage them to play their own role in managing the community to which they belong.

### III. Safer Social Networking Principles

#### ***Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner***

Providers should create clear, targeted guidance and educational materials designed to give children and young people the tools, knowledge and skills to navigate their services safely.

These messages should be presented in a prominent, accessible, easy-to-understand and practical format (e.g. on a help pages and/or in locations where the user makes a decision about how to use the service).

Service providers should provide clear information about what constitutes inappropriate behaviour. This information should be easily accessible and include information about the consequences of breaching these terms. Providers should explore other ways to communicate this information outside of the Terms of Service.

Parents play a crucial role in their child's internet safety and this role is often best fulfilled when a parent is able to discuss safety issues with their child in an open and informed way. As such, providers should offer parents targeted links, educational materials and other technical controls as appropriate with the aim of fostering dialogue, trust and involvement between parents and children about responsible and safer internet use.

Teachers and other carers also play a crucial role in promoting the safe use of SNSs by children and SNS providers should ensure that such materials also empower teachers to help children use SNSs safely and responsibly.

#### ***Principle 2: Work towards ensuring that services are age-appropriate for the intended audience<sup>9</sup>***

Providers should, in the normal course of developing and managing SNSs, consider how their service may be associated with potential risks to children and young people, where it is intended for them to use the service<sup>10-11</sup>. Service providers should seek to limit exposure to potentially inappropriate content and contact. Measures that are available or appropriate to each service will vary in each case<sup>12</sup>, but may include for example:

- making clear when services are not appropriate for children and young people or where a minimum registration age applies;

---

<sup>9</sup> The intended audience as outlined in each providers' Terms of Service

<sup>10</sup> The intended audience as outlined in each providers' Terms of Service

<sup>11</sup> Each SNS is different in terms of target audience, the range of activities users can engage in, the platforms on which they can be consumed and the countries in which they are available. These factors will affect the range and extent of the risks that may affect children and young people when using the site. Assessments of what constitutes inappropriate content for children and young people also varies.

<sup>12</sup> The same combination of factors as listed in the previous footnote will determine what measures are appropriate to address the unique set of challenges and potential risks to users on a particular service. In addition, service providers may also be required to comply with specific local legal requirements pertaining to children's privacy, which may affect how the service is operated in any given jurisdiction. For example, it is common for US-based service providers to adopt a minimum age of 13 years for their services. This reflects the requirements of the Children's Online Privacy Protection Act (COPPA), which only allows providers to collect data without parental consent from users over 13 years old. In the absence of specific local legal requirements, however, service providers will adopt a default specification for their product which is determined by a range of factors such as company policy, adherence to industry good practice or the prevailing law in their principal market.

- taking steps to identify and delete under-age users from their services;
- taking steps to prevent users from attempting to re-register with a different age if they have previously been rejected for being below the minimum age (if their Terms require a minimum age), such as employing cookies;
- working within technical and legal constraints to promote compliance with minimum age requirements;
- promoting the uptake of parental controls which allow parents to manage their children's use of the service;
- providing the means for content providers, partners or users to label, rate or age restrict content where appropriate<sup>13</sup>;
- only showing certain professionally produced content certain times of the day.

### ***Principle 3: Empower users through tools and technology***

Providers should employ tools and technologies to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted (but not illegal) content or conduct. Service providers should make an assessment of what measures to implement based on the services being offered and the intended audience.

The measures that can help minimise the risk of unwanted or inappropriate contact between children and young people and adults may include for example:

- taking steps to ensure that private profiles of users registered as under the age of 18<sup>14</sup> are not searchable;
- setting the default for full profiles to 'private' or to the user's approved contact list for those registering under the age of 18<sup>15</sup> (some service providers set the profile default as 'private' for all users);
- ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list (users may actively choose to change their settings to public or equivalent);
- giving users control over who can access their full profile by, for example, being able to block a user from viewing their profile and 'reject' friend requests;

---

<sup>13</sup> For example, the Broadband Stakeholder Group's good practice principles on audiovisual content information. See <http://www.audiovisualcontent.org/>

<sup>14</sup> The 18+ age requirements may be difficult for services that have already been developed around the legal age of consent, e.g. 16 years. However, future services should consider using 18 years.

<sup>15</sup> The 18+ age requirements may be difficult for services that have already been developed around the legal age of consent, e.g. 16 years. However, future services should consider using 18 years



- giving users the option to allow only direct friends to post comments and content to their profile or to delete unwanted comments;
- giving users the option to pre-moderate comments of other users before being published on their profile;
- providing easy-to-use tools for users to report inappropriate contact from or conduct by another user;
- educating parents about available tools, both for wider internet access (for example, the benefits of using filtering tools and/or parental controls<sup>16</sup>) and the tools, information and advice provided to parents by social networking sites to help them protect young people.

***Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service***

Providers should provide a mechanism for reporting inappropriate content, contact or behaviour as outlined in their Terms of Service, acceptable use policy and/or community guidelines. These mechanisms should be easily accessible to users at all times and the procedure should be easily understandable and age-appropriate.

Reports should be acknowledged and acted upon expeditiously.

Users should be provided with the information they need to make an effective report and, where appropriate, an indication of how reports are typically handled.

***Principle 5: Respond to notifications of illegal content or conduct***

Upon receipt of notification of alleged illegal content or conduct<sup>17</sup> providers should have effective processes in place to expeditiously review and remove offending content.

Service providers should have in place arrangements to share reports of illegal content or conduct with the relevant law enforcement bodies and/or hotlines. These arrangements will depend on local jurisdiction and applicable law, as well as the existence of effective reporting frameworks.

Providers may consider including links to other local agencies or organisations, for example the relevant InHope services and law enforcement agencies. Where there is an immediate threat to safety or life users should be advised to contact the emergency services by, for example, phoning 999 (UK) or 112 (EU).

---

<sup>16</sup> See some of the solutions at “Study on Safer Internet Programme BENCHmarking of Filtering software and services” at <http://www.sip-bench.eu/index.html>

<sup>17</sup> In the context of child protection, illegal content and conduct in this context refers to child abuse images and grooming respectively.

***Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy***

Providers should provide a range of privacy setting options with supporting information that encourages users to make informed decisions about the information they post online. These options should be prominent in the user experience and accessible at all times<sup>18</sup>.

Providers should consider the implications of automatically mapping information provided during registration onto profiles, make users aware when this happens, and should consider allowing them to edit and make public/private that information where appropriate.

Users should be able to view their privacy status or settings at any given time. Where possible, the user's privacy settings should be visible at all times.

***Principle 7: Assess the means for reviewing illegal or prohibited<sup>19</sup> content/conduct***

SNS providers should, during the normal course of developing and managing SNSs, assess their service to identify potential risks to children and young people in order to determine appropriate procedures for reviewing reports of images, videos and text that may contain illegal and inappropriate/unacceptable/prohibited content and/or conduct.

There is a range of procedures which can be used to promote compliance with the Terms of Service, Acceptable Use Policy and/or House Rules. These may include for example:

- human and/or automated forms of moderation;
- technical tools (e.g. filters) to flag potentially illegal or prohibited content;
- community alerts;
- user-generated reports.

Some providers employ human moderators who interact in real-time with children or young people. Such providers should take reasonable steps (working within good practice frameworks<sup>20</sup> where possible or legal frameworks as applicable), to minimise the risk of employing candidates who may be unsuitable for work which involves real-time contact with children or young people.

---

<sup>18</sup> Social networks are used for myriad purposes and by a wide range of users. Different services have different profile formats which allow users to share different information about themselves, for example some providers encourage users to create nicknames and post avatars and create a novel online identity. These formats vary between sites.

<sup>19</sup> Prohibited content/conduct as defined by Terms of Service, Acceptable Use Policy and/or House Rules

<sup>20</sup> Home Office Internet Task Force Good Practice Guidance for the Moderation of Interactive Services for Children <http://police.homeoffice.gov.uk/publications/operational-policing/moderation-document-final.pdf>

## IV. Evaluating the Safer Social Networking Principles

Providers supporting these Principles are committed to implementing safety practices and support all seven Principles outlined in this document. These providers will assess the risk of potential for harm to children and young people on their service, and will consider the application of the specific recommendations outlined in this document accordingly.

- In the interests of transparency, these providers will self-declare<sup>21</sup> how they have considered the Principles which are relevant to their services. These providers will provide the European Commission with this self-declaration.
- Providers will make available for publication non-confidential information from their declaration about their consideration of these Principles.
- Providers supporting these Principles will reconvene after eighteen months with other stakeholders to:
  - Review trends in safety policies and practices.
  - Update stakeholders on the evolution of communication technologies.
  - Review user behaviour and associated risks to users.
  - Review and revise the document where appropriate to ensure that it remains relevant and up-to-date and that it reflects developments in online safety practice.
  - Assess the effectiveness of the document.
- Providers supporting these Principles and other stakeholders will work together to encourage other social networking service providers to add their support to this document and its objectives. They will also endeavour to raise awareness of these goals more widely to interested stakeholders, including users.

---

<sup>21</sup> A common self-declaration format will be developed and used by all providers.

## V. Annex I

### *Explanatory note on how these Principles may apply to applications*

As outlined in the introduction, applications are increasingly a feature of SNSs. There are three categories of applications, which are broadly defined by the relationship that exists between the application and the SNS. This relationship determines how a provider can apply these Principles, as follows:

1. Applications which are pre-installed, integral to or hosted and sponsored by a SNS and made available by the SNS provider. In these instances, there may be a relationship between the SNS and the application developer. In the context of this category of applications, providers should consider the following:
  - undertake a risk assessment of the potential for harm to children and young people, the goal being compliance with the site's policies and safety and security good practice guidelines;
  - include relevant advice for children and young people in educational material (e.g. 'Help pages');
  - respond appropriately upon receipt of reports regarding an application's non-compliance with the site's policies.
  
2. Applications which have been created by third party developers and which are displayed on the SNS's Open API platform. The SNS's users can choose to install these applications on their profiles. There is generally a limited relationship between the SNS and the application developer in this instance. In the context of this category of applications, providers should consider the following:
  - make reasonable efforts to raise awareness among third party developers of industry good practice (which includes these Principles and similar initiatives);
  - include relevant advice for children and young people in educational material (e.g. 'Help pages') and make users aware that a third party application may not afford the same protections as users expect on the SNS in question;
  - upon receipt of notification that an application available to children and young people is in breach of the provider's policies, SNS providers will, where appropriate, notify the developer of the situation, and at all times reserve the right to take down applications which break the provider's policies.

3. Applications which are available from a gallery of third party applications on a platform other than the SNS provider's platform. Users can choose to install these applications on their SNS profile. There is typically no relationship between the SNS and the application developer in this instance. In the context of this category of applications signatory companies should consider the following:
- include relevant advice for children and young people in educational material (e.g. 'Help pages') and make users aware that a third party developer may not afford the same protections as the SNS in question;
  - upon receipt of notification that an application available to children and young people is in breach of the provider's policies, SNS providers will, where appropriate and possible remove the link to the application.

## **EXAMPLES OF AUSTRALIAN CYBER-SAFETY AND YOUTH OUTREACH INITIATIVES**

### **Cyber-safety Initiatives**

- The Australian Government's Cyber-safety Plan which includes:
  - the formation of the Youth Advisory Group and its associated website, *y@g Online*; and
  - the work by the Australian Communications and Media Authority to develop a cyber-safety schools 'gateway' which will support a whole school approach to cyber-safety.
- The Australian Federal Police's *Today's Youth Forum* which provides an interactive site through MySpace and focuses on cyber-safety issues.
- The *SuperClubsPlus Australia* social networking site funded by the Telstra Foundation.
- The Alannah and Madeline Foundation's *CyberSmart Campaign*: a proposed system to accredit primary and secondary schools that have policies in place that encourage the use of technologies such as the internet and mobile phones in safe and responsible ways.

### **Outreach, which may include cyber-safety topics**

- The *Cybersmart Kids Online* site, hosted by ACMA.
- The *ThinkUKnow* site, hosted by the AFP and Microsoft.
- The *Australian Youth Forum*, announced by the Minister for Youth Affairs, the Hon Kate Ellis MP, which includes an interactive site.
- The *Bullying. No way!* site: has an interactive component and a section on cyber-bullying—created by Australia's educational communities (State, Territory and Commonwealth government education departments, and Catholic and independent education sectors).
- The *Kids Help Line*, which provides free, confidential and anonymous, telephone and online counseling services for young people aged between 5 and 25.
- The *Smart Online Safe Offline* program of the National Association for Prevention of Child Abuse and Neglect, designed to teach children aged 9 to 14 years to stay safe online as well as providing support for parents, teachers and the community.
- Centacare Sandhurst's *Loddon Mallee Cyber Safety program*, a Bendigo-based not-for-profit organisation with a rural and provincial focus.
- Edith Cowan University in Western Australia's *Child Health Promotion Research Centre*, which is developing a parent education program that will test educational strategies designed to help parents increase their child's cyber safety.
- The New South Wales Youth Advisory Council (YAC) set up to advise the NSW Government on issues of concern to young people (aged 12-25) in NSW, Government policies relating to young people, and youth-related programs.
- The *Queensland Youth Council*, which provides a forum for the exchange of information and views between young people and the Queensland Government.

## **ATTACHMENT E**

- The *Student Youth Network* in Melbourne, which will get a small team of its young volunteer reporters to research and discuss cyber safety on its radio and television stations and online.
- The Child Health Promotion Research Centre's (Edith Cowan University) *Parent Education Program*, providing parents with support and advice on how to deal with cyber safety.
- Australian Institute of Criminology's publication, *Cyber-bullying issues for policy makers*, No. 59, 2007.
- Mental Health Association NSW Inc's Fact Sheet, *Cyber Bullying*, 2008.

YouTube safety and integrity elements

YouTube is a user-generated video sharing platform around which communities form, have discussion and interact. Google's efforts to maintain the safety and integrity of YouTube comprise four primary elements:

1. Clear policies regarding what is and is not acceptable
  - All users of YouTube must abide by the terms of use and the [YouTube Community Guidelines](#), which are written in easy-to-understand language and provide users with clear rules on what content and behavior is acceptable and what is not.
2. Robust enforcement mechanisms for these policies.
  - Every minute, 24 hours of video are uploaded to YouTube. As a platform for user-generated content, and given the volume of content, it is not possible to review videos in advance of them being made available on the site.
  - YouTube has developed a reliable and user-friendly community policing system - users [report](#) potential violations of the YouTube Community Guidelines by "flagging" a video, flagged videos are then reviewed for compliance with the Community Guidelines 24 hours a day, seven days a week.
  - The YouTube review teams receive extensive training on an ongoing basis, including from law enforcement organisations and child safety organisations. This training enables the team to effectively and efficiently respond to flagged videos.
  - Where a video does not comply with the Community Guidelines, it will be removed from the site. When a video is removed, the user is advised and sent some tips to remind them of the rules regarding what content can be posted to YouTube. In appropriate circumstances, YouTube will refer the matter to law enforcement.
  - Users who repeatedly violate the YouTube Community Guidelines have their accounts terminated.
  - YouTube has also developed digital hashing technologies to prevent the re-upload of files that have been removed, and is continually developing tools to promote this goal.
  - In addition to the flagging system, users are able to contact YouTube directly with privacy, harassment, or bullying complaints through the [Help & Safety Tool](#).
3. Innovative product features that enable safer behavior.



## **ATTACHMENT F**

- [Safety Mode on YouTube](#) is an opt-in setting that helps screen out potentially objectionable content that a user may prefer not to see or don't want others in their family to stumble across while enjoying YouTube.
  - Users are empowered to manage their own experience by:
    - uploading videos as “Private” to be shared with specified family and friends
    - blocking specific users from interacting with them
    - choosing to allow only their “friends” to communicate with them
    - choosing to pre-screen comments
    - choosing to disable commenting altogether for each of their videos
    - choosing to filter the comments they see. This gives users the control to set their preferences so that they see only filtered comments.
4. Education to increase user awareness of how to stay safe.

The [YouTube Safety Centre](#) provides multimedia safety tips to users, including advice on keeping personal videos private, cyberbullying, spam and phishing; as well as information about how to protect their identity and appropriately manage interactions with other users, and tips on how to be a responsible cyber citizen and how to use the community flagging system.