14

Australian responses to cyber-safety issues

14.1 Australia's response to cyber-safety issues has been largely educational. International responses to cyber-safety issues will be set out in Chapter 15.

Australian Government responses

14.2 Responses to the range of cyber-safety issues are fragmented across agencies and jurisdictions.

Australian Communications and Media Authority

14.3 The Australian Communications and Media Authority (ACMA) is located within the Department of Broadband, Communications and the Digital Economy. It is responsible for the regulation of broadcasting, radio-communications, telecommunications and online content. This includes the Internet, radio and TV, phones and licences for consumers and industry.

14.4 ACMA has a range of important, free resources in place to improve cyber-safety: a Cyber Safety Help Button was launched at the end of 2010, while a collection of programs has been in operation for some time.

14.5 Since 2000, it has undertaken a sequence of research projects exploring children's use of online technologies, with a focus on the home environment.[1]

14.6 It has also conducted a three-year program of research examining developments in safety initiatives around the world aimed at protecting both minors and adults.[2]

---

1 Australian Communications and Media Authority, *Submission 80*, pp. 3-5.

14.7 In addition to its research and promotional activities, ACMA has other resources :

- The *Cybersmart* website and the suite of education resources for young people and teachers contained on that site;
- Professional Development for Educators;
- Internet Safety Awareness Presentations for students, parents and teachers;
- Pre-service teacher training program; and
- The public libraries suite of resources.[3]

14.8 As already noted, at the National Day of Action Against Bullying and Violence on 18 March 2011, it staged a national *Cybersmart Hero* event created to tackle cyber-bullying. This is a one-hour, in-school, on-line activity for students in Years 5 and 6 that addresses the responsibilities of the people in the best position to influence bullying and cyber-bullying: the bystanders.

14.9 On 18 March, ACMA also provided a suite of lesson plans for teachers on how to prevent and manage cyber-bullying. These plans bring the discussion into the open, and encourage students to tell their parents/carers or teachers when they are aware of cyber-bullying.[4]

14.10 Under the *Broadcasting Services Act 1992* (Cth), ACMA has the regulatory responsibility for a hotline where complaints can be made about offensive and inappropriate content. It has observed a 'steady increase' in the number of complaints, particularly relating to online child abuse and child sexual abuse material hosted overseas.[5] It is the primary agency for removing online content and works with the Australian Federal Police (AFP), which assess information to decide whether there should be an investigation. If a website is hosted offshore, these authorities are limited in what they can do.[6]

14.11 Roar Educate commented that ACMA's predominant resources were derived from the United Kingdom's Child Exploitation and Online Protection Centre, and have been available for 'five or six years'. [7]

2 Australian Communications and Media Authority, *Submission 80*, p. 2.

3 Australian Communications and Media Authority, *Submission 80*, p. 5.

4 *acma(sphere*, Issue 62, April 2011, p. 6.

5 Australian Communications and Media Authority, *Submission 80*, p. 8.

6 Australian Communications and Media Authority, *Submission 80*, p. 8; Australian Federal Police, *Submission 64*, p. 7.

7 Mr Craig Dow Sainter, Managing Director, Roar Educate, *Transcript of Evidence*, 20 April 2011, pp. CS28-29.

Cybersmart programs

14.12 ACMA pointed out that its research programs had been progressively redesigned to incorporate the views of children and young people, with findings indicating that issues such as cyber-bullying have been of increasing concern. *Click and Connect: Young Australians' use of online social media* sought to understand the extent to which young people use social networking and their experiences in dealing with risks online.[8]

14.13 The Cybersmart website is the cornerstone of ACMA's *Cybersmart* program. It acts as a 'one-stop' shop for general cyber-safety information, with information targeted to six specific audiences:

- 'young children' (not defined);
- children;
- teenagers;
- parents;
- teachers; and
- librarians.[9]

14.14 Under the *Cybersmart* brand, ACMA delivers a 'diverse, comprehensive and effective range' of programs and resources tailored to meet the needs of teachers, parents/carers, librarians and young people.[10] These programs have proven to be 'extremely popular' and continue to be in high demand.[11]

14.15 It noted that online safety messaging had generally assumed that any degree of risk was negative, while emerging research suggested that a certain level of risk taking was necessary for the development of resilience in young people.[12] Its research programs had therefore been progressively redesigned to incorporate the views and experiences of young people.

14.16 Since 2009:

- There have been 2,335 separate Internet Safety Awareness presentations and professional development workshops, with participants from over 3,300 schools;

8 Ms Andree Wright, Acting General Manager, Digital Economy Division, *Transcript of Evidence*, 3 March 2011, p. CS3.

9 Australian Communications and Media Authority, *Submission 80*, p. 21.

10 Australian Communications and Media Authority, *Submission 80*, p. 1.

11 Australian Communications and Media Authority, *Submission 80*, p. 1.

12 Australian Communications and Media Authority, *Submission 80*, p. 6.

- 263,000-plus teachers, students and parents have attended one hour general Internet safety awareness presentations;
- Over 7,500 teachers have participated in free full-day professional development workshops;
- There have been 6.6 million page views of the *Cybersmart* website; and
- More than 2.6 million hard copy *Cybersmart* resources have been distributed to schools, community groups and families across Australia.[13]

14.17 ACMA noted that its resources continued to be in 'high demand', and were 'widely acknowledged' as based on evidence and world–class. Tributes were paid to the quality and range of its material.[14]

Cybersafety Help Button

14.18 The Cybersafety Help Button launched on 10 December 2010 was developed in response to advice from the Youth Advisory Group. This body said that it would like a 'one-stop-shop' for cyber-safety advice and assistance.[15] The Button provides users, particularly children and young people but also parents/carers and teachers, with easy online access to a wide range of cyber-safety and security resources to help with cyber-bullying, unwanted contacts, scams, frauds and inappropriate material.[16]

14.19 The Department of Broadband, Communications and the Digital Economy commented that:

> We have taken very seriously the advice that the children have given us. Indeed, the button was as a result of their advice. They said, 'Look, it's all bewildering. We don't know where to go. You can't expect us to remember all these government websites. They're changing all the time. We're confused. We want a one-stop shop. Make it easier for us so that we can press the one button

13 Ms Andree Wright, Acting General Manager, Digital Economy Division, *Transcript of Evidence*, 3 March 2011, p. CS3.

14 Ms Andree Wright, Acting General Manager, Digital Economy Division, *Transcript of Evidence*, 3 March 2011, p. CS4.

15 Australian Government's Consultative Working Group on CyberSafety, *Submission 113*, p. 7.

16 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS2.

> and go to all the sites that are relevant. That would make life a lot easier.' So we proceeded to develop the button.[17]

14.20 This Help Button is based around three actions that a user can take if there are concerns about material online:

- talking to a professional, either over the phone or online;
- reporting matters that may be of concern to a range of agencies; and
- learning about cyber-safety.

14.21 There are also proposals to extend the features of the Help Button. For example, social networking site and games that are popular with children have conditions of use which are long, detailed and legalistic:

> It is very difficult for a 12-year-old to try to understand all of that legalistic language. More often than not, they will just scroll to the bottom of the page and click 'I Agree' and then proceed, and they will not read it. But they are saying, 'Sometimes I am clicking yes to something and I have no idea what I'm doing but, because my mate did it ... they were looking for was some easy way in which they could understand the key features of each of the different social networking sites and popular games: some really simple, attractive format. So we are looking to add as a feature of the button an ability for children—and, indeed, parents and teachers, if they wish—to find out about the latest game or the latest social networking site and what the key features of it are and what they need to understand about it. That will, I think, assist both children and parents when they make the decision about it. It is an often difficult decision when the child says, 'I want to play this' or 'I want to go on that. Am I allowed?' and the parent says, 'I am not sure. I don't know what you're talking about.' This may help parents by providing them with some sort of guide in that regard.[18]

14.22 While user downloads continue to increase, numbers do not accurately reflect actual usage, as the Help Button can be downloaded once and applied to multiple sites or computers.

---

17 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS22.

18 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS22-23.

14.23 The Department is seeking to expand progressively what is behind the three actions already on the Help Button. Work has also begun on a second stage that will include an application compatible with mobile platforms and browser-level applications. This work is expected to be completed in the second half of 2011. It is also intended to add advice on the range of options that are available about localised filtering systems.[19]

14.24 Promoted by members of the Consultative Working Group on Cybersafety, the Help Button has been downloaded by the Queensland Department of Education and Training across its network and is available on over 177,000 computers in that State. There are, therefore, 'at least 200,000' of these Buttons on a range of computers around Australia. Other State/Territory school systems have been encouraged to adopt the Help Button, as have libraries.[20]

14.25 BraveHearts believes that online reporting systems are important tools in responding to child exploitation. The use of hotlines provided an alternative to reporting to law enforcement agencies to which people may be reluctant to report illegal content.[21]

14.26 The South Australian Office for Youth was critical of the Help Button because it believed that, although there is a button to report matters online, it goes to a page that is not 'very user friendly'. While it might be downloaded by parents/carers, doubts were expressed that young people would download or use it.[22]

Consultative Working Group on Cybersafety

14.27 The Consultative Working Group on Cybersafety is an initiative of the Government's Cybersafety Plan. It includes representatives of industry and community organisations, and Australian government agencies. Chaired by a senior officer of the Department of Broadband, Communications and the Digital Economy, its roles are to:

- Consider all aspects of cyber-safety faced by Australian children;

19 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, pp. CS2-3, 21, 23.

20 Ms Patrea Walton, Acting Deputy Director-General, Department of Education and Training, Queensland, *Transcript of Evidence*, 17 March 2011, p. CS80; Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy, *Transcript of Evidence*, 3 March 2011, p. CS17.

21 BraveHearts, *Submission 34*, p. 11.

22 Mrs Tiffany Downing, Director, Office for Youth SA, *Transcript of Evidence*, 3 February 2011, p. CS24.

- Provide information to Government on measures required to operate and maintain world best practice safeguards for Australian children in the digital economy; and
- Advise the Government on priorities for action by government and industry.[23]

14.28 The Working Group's Terms of Reference specify six areas of focus:

- The online environment in which Australian children currently engage;
- The nature, prevalence and implications of cyber-safety risks;
- Australian and international responses to current cyber-safety risks;
- Opportunities for cooperation across Australian and international stakeholders;
- Information required to realise the potential for achieving and continuing world's best practice of safeguards; and
- Ensuring that the Group's deliberations take account of new technologies.[24]

Department of Education, Employment and Workplace Relations

14.29 The Department of Education, Employment and Workplace Relations (DEEWR) pursues activities based on the knowledge that the well-being and safety of children and young people at school is essential for their academic development, and for that nation's ongoing economic prosperity and social cohesion.[25]

14.30 The National Safe Schools Framework was originally endorsed by all Australian Ministers for Education in 2003. It included an agreed 'set of national principles to promote safe and supportive school environments, and appropriate responses to address bullying, harassment, violence, child abuse and neglect'.[26]

14.31 Consultations have indicated that the National Safe Schools Framework has been an effective vehicle for raising community awareness of safe school environments. It has 'promulgated a greater understanding and

23 Australian Government's Consultative Working Group on CyberSafety, *Submission 113*, p. 1.
24 Australian Government's Consultative Working Group on CyberSafety, *Submission 113*, p. 1.
25 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 4.
26 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 7.

appreciation of the relationship between such environments, student well-being and improved learning'.[27]

14.32 Following a review in 2009, a revised Framework was endorsed in 2010 and launched on 18 March 2011, to coincide with the National Day of Action Against Bullying and Violence. The revised National Safe Schools Framework will be distributed to all primary and secondary schools.[28]

14.33 The Australian Government and State/Territory education authorities are represented on the Safe and Supportive Schools Communities project management group. This is a cross-jurisdictional forum enabling identification of emerging 'national priorities, sharing of knowledge and exchange of effective, evidence-based practice'.[29]

14.34 This project collaborated in developing a nationally agreed definition of bullying which has been included in the revised National Safe Schools Framework. It is intended to use this definition in relevant policies and guidelines.

14.35 DEEWR provides funding and other support for a range of programs and initiatives, including the seven general capabilities to be addressed in the Australian curriculum:

- Literacy;
- Numeracy;
- ICT competence;
- Critical and creative thinking;
- Ethical behaviour;
- Personal and social competence; and
- Inter-cultural understanding.[30]

14.36 The safety of young people in the online environment is paramount, and $125.8 million has been allocated for a comprehensive Cybersafety Plan that includes:

- $49 million over four years to the AFP Child Protection Operations Team for detection and investigation of online child sex exploitation;

27 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 7.
28 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 8.
29 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 14.
30 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 9.

- $42.4 million over four years to develop and implement Internet service provider-level filtering;
- $11.9 million to ACMA to implement a comprehensive range of education and outreach activities; and
- $4.3. million to ACMA over four years to develop a new cyber-safety website with up-to-date and age-appropriate educational material, and to improve the online helpline to provide a quick and easy way for children to report online incidents that cause them concern.[31]

14.37 This Plan also recognises the value of young Australians providing advice to Government on cyber-safety issues by providing $3.7 million over four years to the Youth Advisory Group and its online forum.[32]

Attorney-General's Department

14.38 The Attorney-General's Department has released the *Protecting Yourself online – What everyone needs to know* pamphlet and has distributed 270,000 copies.[33] The *ID Theft – Protecting your Identity* booklet has had 60,000 copies distributed.[34]

14.39 The Australian Education Union encouraged greater interagency collaboration and made the point that:

> It is clear therefore that there is no shortage of effort going into policy responses to issues of cyber-safety but perhaps there is evidence of a need for greater inter-agency cooperation (given programs and policies are being released under the auspices of the Department of Broadband, Communications and the Digital Economy, the Attorney General, and to education departments) and for better engagement between schools and working within the broader community.[35]

State and Territory Government responsibilities

14.40 Authorities in the Australian States and Territories have a range of responsibilities and programs designed to make young people safe in the

31 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 11.
32 Department of Education, Employment and Workplace Relations, *Submission 135*, p. 11.
33 Attorney-General's Department, *Submission 58.1*, p. 1.
34 Attorney-General's Department, *Submission 58.1*, p. 1.
35 Australian Education Union, *Submission 11*, pp. 7, 9.

online environment. The submission from the Consultative Working Group on Cybersafety gave details of State/Territory programs to develop cyber-safety educational programs.[36]

New South Wales

Education

14.41 Internet and online communication services are provided in NSW schools by the Department of Education and Training for research and learning and communication between students and staff. Access to the online environment assists students to develop the skills necessary for effective and appropriate use of the Internet. It also provides a context for learning about roles and responsibilities in communication, respectful relationships and personal safety.[37]

14.42 The *KidsMatter* and *MindMatters* initiatives have both been informed by, and have informed, the development of the National Safe Schools Framework, with bullying and harassment as one of its target areas.[38] Since 2007, cyber-safety has been the focus of the bullying and harassment arm of the project. It has trained 130,000 people across the country and reached 1,500 secondary schools since 2000.[39]

14.43 The Department's *Online Communication Services: Acceptable Usage for School Students* policy includes access and security, privacy and confidentiality, intellectual property and copyright, as well as misuse and breaches of acceptable use of technology.[40] As part of the curriculum, students also receive instruction in these issues.

14.44 Under an 'Acceptable Use' policy, students are aware that:

- they are responsible for their actions while using the Internet and online communication services, and

36 Australian Government's Consultative Working Group on CyberSafety, *Submission 113*, pp. 3-4.

37 NSW Government, *Submission 94*, pp. 2-3

38 NSW Government, *Submission 94*, pp. 23-24.

39 Mr Jeremy Hurley, Manager, National Education Agenda, Principals Australia, *Transcript of Evidence*, 11 June 2010, p. CS8.

40 NSW Government, *Submission 94*, p. 3.

- the misuse of Internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.[41]

14.45 Students are asked to report any Internet sites accessed that are considered to be inappropriate, as well as any suspected security breach from other schools, TAFE or from outside the Department.[42]

14.46 Senior students in NSW schools have access to the *Digital Education Revolution-NSW* wireless network in schools. Their laptops can connect anywhere students collaborate, study and learn. This wireless network provides a secure online environment. Laptops are subject to a strict Internet filtering policy and any site not recognised is blocked, including so-called proxy sites that enable users to by-pass filters.[43]

14.47 A Digital Citizenship education program has been developed that is proposed for implementation in 2011. This is a strategy to teach students the skills to be good digital citizens.

14.48 The Department is also represented on the *Safe and Supportive School Communities* project: a collaborative initiative of Australian governments overseeing the *Bullying, No Way!* website. In support of this initiative, schools are provided with a range of anti-bullying material.[44]

14.49 In partnership with the Department and schools, NSW Community Justice Centres developed a Peer Mediation Program. As one of a broad range of conflict mediation strategies for schools, it was initiated in 1994 as an early intervention strategy offering an effective method of dealing with and resolving some student disputes. The issues and principles raised by cyber-bullying are similar to those encountered in bullying.[45]

14.50 Each NSW school is required to have an anti-bullying policy and, when required, these matters are initially dealt with internally. Police liaison officers address cyber-bullying issues in schools, but an incident only becomes a police responsibility if it involved a criminal offence.[46]

14.51 The Digital Citizenship program includes cyber-bullying as a theme in all years K-10. It promotes the expectation that all students should be active in preventing it, and understand that even single hostile cyber actions can

41 NSW Government, *Submission 94*, p. 3.
42 NSW Government, *Submission 94*, p. 17.
43 NSW Government, *Submission 94*, p. 3.
44 NSW Government, *Submission 94*, p. 17.
45 NSW Government, *Submission 94*, pp. 18-19.
46 NSW Government, *Submission 94*, p. 29.

have a widespread negative impact because of rapid dissemination and the relative permanency of sent messages.[47]

14.52 The Department places advertisements in daily newspapers describing 'cyber bullying', explaining briefly how it occurs, pointing out measures that can be taken to reduce it and listing contacts for assistance.

Victoria

Education

14.53 To maximise the opportunities presented by new technologies for teaching and learning, the Victorian Department of Education and Early Childhood Development is developing the *KnowledgeBank: Next generation* portal. This will provide a range of quality assured and targeted digital resources for teaching and learning. It will also evaluate and research innovative ways to use new technologies that suited the way students learn, collaborate and network.[48]

14.54 As part of the Government's Respect Agenda, the Department is also developing and would implement a *Respect in Schools* strategy that includes advice on dealing with bullying and Cyber-bullying. This strategy also includes reviewing the *Safe Schools are Effective Schools* policy, with a view to replacing it with: *Building Respectful and Safe Schools*.[49]

14.55 The Learning On Line website presented advice for schools on cyber-safety and the responsible use of digital technologies. It had been developed to help schools make the most of the opportunities presented by developments in, and increased accessibility of these technologies. It also sought to support students using the online environment by minimising risks that may arise.[50]

14.56 The Learning on Line Cybersafety pilot program focused on developing children's ability to act safely and responsibly in the online world, and to prepare them effectively to protect themselves online so they can resolve issues that may arise.[51]

14.57 The pilot program is aimed at three levels:

47 NSW Government, *Submission 94*, p. 9.
48 Victorian Government, *Submission 112*, p. 1.
49 Victorian Government, *Submission 112*, p. 2.
50 Victorian Government, *Submission 112*, p. 2.
51 Victorian Government, *Submission 112*, pp. 2-3.

- Years 3 and 4 - Cybersmart: What does it mean to be cybersmart?
- Years 5 and 6 – Shout Out, Make a Difference.
- Years 7 to 10 – Bystanders: What action can I take?[52]

14.58 The Youth Central website is an initiative for young people aged from 12 to 25 which devoted a section to 'Cyber Smarts'. It included guidelines on how to protect young people from cyber-bullying, tips for keeping the 'person/private' balance, and how to be cyber-safe.[53]

14.59 In its 2010/2011 Budget, the Victorian Government committed $3.6 million to enable six community-based organisations to extend their cyber-safety education programs to more school age children, particularly those from diverse or marginalised backgrounds who are often at risk of bullying behaviour. It will fund those organisations to develop young leaders to work with their peers to help reduce this behaviour, and minimise its impact, by giving vulnerable young people the skills to keep themselves safe online.[54]

14.60 In October 2009, the Department convened the Leading Responsibility in a Digital World student summit, attended by 230 Year 10 students. It facilitated discussions between adults and the young people about the issues associated with the online environment. Students summarised the day's thoughts and declared each school's commitment to take action and lead in this environment.[55]

14.61 The Youth Affairs Council Victoria is a not-for-profit organisation funded by the Victorian Government. It has hosted events that bring together young people, teachers, service providers and researchers to examine the prevalence and impact of bullying in the State. It looked for ideas for interventions and solutions, via such forums as *The Sticks and Stones and Mobile Phones – Bullying in the New Millennium*, hosted in August 2009.[56]

14.62 The Department is an active member of, and contributes financially to, the national *Safe and Supportive School communities: Finding Workable solutions for countering bullying, harassment and violence in schools* project for the Australian Education, Early Childhood Development and Youth Affairs Senior Official's Committee.[57]

---

52 Victorian Government, *Submission 112*, p. 3.
53 Victorian Government, *Submission 112*, p. 3.
54 Victorian Government, *Submission 112*, pp. 3-4.
55 Victorian Government, *Submission 112*, p. 4.
56 Victorian Government, *Submission 112*, p. 4.
57 Victorian Government, *Submission 112*, p. 5.

14.63 This is the only national project bringing representatives together from all Australian educational jurisdictions to create safer schools free from bullying, harassment and violence. The 'well-known, respected and comprehensive' website *Bullying, No Way!* is an important result of this project.[58]

14.64 In 2010/2011, the project will focus on strategic support for implementation of the National Safe Schools Framework and related national priorities with a range of activities.

14.65 Victoria actively supports the Alannah and Madeline Foundation and, in 2009, contributed $250,000 to its *Cyber Safety and Wellbeing* pilot program, now known as the *eSmart* program. This will contribute to ensuring children benefit from the learning opportunities provided by the online environment in a safe way.[59]

Queensland

Education

14.66 The Queensland Department of Education and Training has built a safe and secure online learning environment that all students can access from their homes. They are able to use blogs and a range of resources, as well as engage with other students through online forums. A great deal of work has been done to ensure that staff, students and parents/carers are more aware of cyber-safety and the responsible use of technology. The Department will ensure that important messages about cyber-safety continue to be shared and reinforced in school communities.[60]

14.67 In 2010, it established the Queensland Schools Alliance Against Violence. This is a group of key stakeholders, including representatives from the State, Catholic and Independent school sectors, parents/carers, Principals' associations, unions and the Commission for Children and Young People and Child Guardian. Its purpose was to provide advice on best practice to deal with bullying, cyber-bullying and violence.[61]

14.68 The Alliance's report has been used to develop resources for use in all schools in the State. These included:

58 Victorian Government, *Submission 112*, p. 4.

59 Victorian Government, *Submission 112*, p. 5.

60 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, pp. CS79-80.

61 Ms Anita Smith, Senior Education Officer, Student Wellbeing, Learning and Teaching, Services, Brisbane Catholic Education, *Transcript of Evidence*, 17 March 2011, p. CS25.

- a *Declaration against Bullying and Violence;*
- toolkits for schools and for parents, and
- a starter kit for developing local community alliances against bullying and violence.[62]

14.69 Work that has been based on the report's recommendations will be reviewed in about September 2012.

14.70 Students were consulted about bullying, and recommendations made by Professor Ken Rigby of were used to advise schools about tackling bullying and cyber-bullying. In 2010, Dr Michael Carr-Gregg undertook 'a large number' of valuable workshops in ten locations across the State to support and provide advice to parents/carers, teachers and school leavers about bullying and cyber-bullying. He has continued to give these workshops in 2011.[63]

14.71 The Department will be in partnership with the Alannah and Madeline Foundation to provide *eSmart* to all State schools. This is a framework that guides schools to make sure that they are doing everything they can to combat cyber-bullying and promote cyber-safety.[64]

14.72 As already noted, ACMA's Help Button has been placed on over 177,000 school-based computers in the State. All schools are required to develop responsible behaviour plans for students, and these had to be reviewed to ensure that they included strategies to deal with bullying and cyber-bullying. The enrolment process includes 'Acceptable Use' agreements with parents/carers about the use of technology by students.[65]

14.73 The Department has a repository of resources around bullying and cyber-bullying, the '*Bullying.No Way!*' website, provided by the Australian Government under the Safe and Supportive Schools Communities project.[66]

---

62 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, pp. CS79-80.

63 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, p. CS80.

64 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, p. CS80.

65 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, p. CS80.

66 Ms Patrea Walton, Acting Deputy Director-General, Queensland Department of Education and Training, *Transcript of Evidence*, 17 March 2011, pp. CS80-81.

South Australia

Education

14.74 The South Australian Department of Education and Children's Services recognised the issue of bullying in 1996 and detailed it in the school discipline policy. School communities are encouraged to work together to create an environment free from harassment and bullying. Since 2005, all Departmental schools have been required to have an anti-bullying policy and they are now also encouraged to have a cyber-bullying emphasis. The non-government education sector has the same requirements.[67]

14.75 It has developed the pre-school to Year 12 package *Keeping Safe: Child Protection Curriculum*, and trained 17,000 of its 20,000 teachers in its use. The Catholic sector in South Australia is implementing it, as are schools in the Northern Territory. It is unique because it connects cyber-safety with child protection, emphasising the importance of implementing the document and teaching respect for relationships. It provides advice on Internet security, including examples of cyber-safety user agreements, and actions principals can take following a cyber-safety event. It also addresses the issue of teachers' digital footprints.[68]

14.76 In May 2009, it advised principals on actions that they can take on cyber-bullying or electronic crime. This clarified their use of disciplinary powers, including suspension and exclusion, for events occurring beyond the school gates and outside school hours where the well being of a student, teacher or member of the school community is affected.[69]

14.77 In 2010, the Department:

- provided $100,000 in grants to schools to implement innovative practices. These are being written up for placement on the Department of Education and Children's Services website; and
- collaborated with the South Australian Police to have cyber-safety as part of the two-yearly primary schools' music extravaganza.[70]

---

67 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, pp. CS66-67.

68 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS68.

69 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS68.

70 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS69.

14.78 In 2005, the South Australian Government formed the Coalition to Decrease Bullying, Harassment and Violence in South Australian schools. Its initiatives have included:

- The 2006 Safer South Australian Schools Conference;
- The pamphlet *Cyber bullying, e-crime and the protection of children and young people*, 150,000 copies of which were distributed to all schools in the State;
- Coordination of National Safe Schools Weeks in 2006 and 2007;
- Providing advice on the National Safe Schools Framework; and
- Support for Dr Barbara Spears of the University of South Australia to gain a grant from the Commonwealth to capture stories from young people, their parents and school staff on cyber-behaviour issues. A web site was developed based on this research. Advice was provided to the school sector, including the Department's policy *Cyber-safety: Keeping Children Safe in a Connected World*.[71]

14.79 Collaboration between the three sectors, public, Catholic and independent, 'is not uncommon' in South Australia, so that a number of child protection documents are policy in all schools in the State.[72] The Department referred to the low rate of bullying in South Australia, noting the suggestion that this was the result of initiatives already undertaken, such as the Coalition mentioned above, and collaboration between the three schooling sectors.

14.80 As part of registration in South Australia, teachers are required to complete *Responding to Abuse and Neglect Education and Care* training, and update this every three years. There are elements of cyber-safety in this training, as it acknowledges that teachers are required to maintain a professional; presence on the Internet. It also addresses the issue of teachers' digital footprints, including those of pre-service teachers who are likely to use social networks more often than older teachers.[73]

South Australian Office for Youth

14.81 In response to a growing concern about the risks to young people associated with using social networking sites, the South Australian Office

71 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, pp. CS67-68

72 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS68.

73 Mr Greg Cox, Senior Policy Advisor, Student Wellbeing, South Australian Department of Education and Children's Services, *Transcript of Evidence*, 3 February 2011, p. CS69.

for Youth ran a Social Networking Education and Awareness Campaign in June 2010.[74]

14.82 The temporary Safer Social Networking info-line was open from 4 to 11pm on two days, seeking:

- to provide young people and their parents/carers with the necessary information to enable a better understanding of, and to set, privacy settings on individuals' social networking sites; and
- to identify key social networking issues for young people.[75]

14.83 An online survey was placed on the Office's website.

14.84 The one-stop-shop Cyber Safety Information Portal provided young people and their parents/carers with a range of information on cyber-safety.

14.85 The info-line received 27 calls, and 103 people responded to the survey. The campaign showed public concern for many of the issues raised in this Inquiry, including some that were not often publicised, such as underage users, hacking, how easy it was to lie about identity online and trusting others without knowing who they were.[76]

14.86 In addition to recording concerns about general privacy and identity theft issues it also revealed two other matters. The first was the need for more education about other issues not often raised, such as:

- Knowing what to do if something happens online;
- Understanding users' rights;
- Understanding that the same rules apply online as in the 'real' world; and
- What parents/carers or grandparents can do if they are concerned about young people's online safety.[77]

14.87 The second matter was enforcement. During the Campaign, the Office referred 13 callers to police or ACMA to investigate cyber-safety threats. Many of these callers had already spoken to the police and felt that their concerns had not been adequately addressed. Others had concerns, e.g. about cyber-bullying or hate pages on Facebook, but did not know who to

74 South Australian Office for Youth, *Submission 98*, p. 1.
75 South Australian Office for Youth, *Submission 98*, p. 1.
76 South Australian Office for Youth, *Submission 98*, p. 6.
77 South Australian Office for Youth, *Submission 98*, p. 4.

contact for assistance. For example, at that time, the Office believed that there was no agency clearly responsible for responding to cyber-safety threats, particularly for young people.[78]

14.88 The Australian Education Union referred to the Coalition to Decrease Bullying, Harassment and Violence in South Australian Schools, commenting that it:

> comprises the 3 main education authorities, (DECS, Catholic Ed and Independent Schools) together with the University of SA. This coalition has produced brochures for families etc on Cyber bullying, e-crime and the protection of children and young people.[79]

Western Australia

Education

14.89 The West Australian Education Department has implemented a tiered approach to filtering Internet access to minimise the risk of student and staff exposure to inappropriate content. It has a central filtering service blocking access to approximately 750,000 sites identified as containing content unsuitable for educational needs. This centrally-managed blacklist is linked to similar services around the world and is updated daily to reflect changes occurring on the Internet.[80]

14.90 Each school has an Internet filter, enabling a further level of Internet access to meet local needs best.

14.91 Computers used on school networks are supplied with pre-configured Internet browser software default settings to block certain actions that might inadvertently lead to sexual content.[81]

14.92 A *Students Online* policy has been introduced for public schools to establish school-based procedures that both protect and inform students, and their parents/carers, about use of Departmental online services. All schools have a local policy all students are required to sign encouraging good practice and appropriate online behaviour. The Department works closely with ACMA, and has promoted its *Cybersmart* initiatives.[82]

78 South Australian Office for Youth, *Submission 98*, p. 4.

79 Australian Education Union, *Submission 11*, p. 10

80 Western Australian Department of Education, *Submission 115*, p. 2.

81 Western Australian Department of Education, *Submission 115*, p. 2.

82 Western Australian Department of Education, *Submission 115*, pp. 2-3.

14.93 The Department accepted that the scale and nature of the Internet was such that no filtering mechanism could offer protection from all inappropriate content in a school. When used with user awareness, agreed operating procedures and adequate supervisory techniques in classrooms, this combination of technologies and practices provides a high level of protection.[83]

14.94 The WA Government supported the Child Health Promotion Research Centre at Edith Cowan University to develop *The Cyber Bullying Formative Study (2007-2008)* to address the rise in Cyber-bullying. This study revealed that few children who had been victims of bullying online would not discuss the issue with parents/carers or teachers for fear of having mobile phones or computers removed, or because they believed that adults were unaware of the problem and did not know how to prevent it.[84]

14.95 It provided $400,000 for the first Youth Summit conducted by the Child Health Promotion Research Centre as part of its 2007/2008 Study. Two summits were held to identify effective and appropriate prevention and management strategies for young people, involving responses coordinated between school and families.[85]

14.96 The first Summit enabled 200 Year 10 students to engage in problem-solving about cyber-bullying. The second was for staff and parents/carers, and the result was a Declaration presented to the Minister. The ideas outlined in this document demonstrated the willingness of young people to own a problem and develop their solutions. It also confirmed 'that student-focussed solving of problems is the most powerful strategy to combat cyber-bullying'.[86]

14.97 A cross-sectoral and inter-agency body, the Cyber Safety for Children Working Party, has been set up, the first in Australia to establish links between stakeholders supporting schools to address online safety issues.[87] It provides a forum for the discussion and application of findings about the nature, prevalence, implications of and level of risk associated with cyber-safety threats, as well as the effectiveness of both Australian and international responses to safety threats.

83 Western Australian Department of Education, *Submission 115*, p. 4.

84 Western Australian Government, *Submission 118*, pp. 3-4.

85 Western Australian Government, *Submission 118*, p. 4.

86 Western Australian Government, *Submission 118*, p. 4.

87 Western Australian Government, *Submission 118*, p. 4.

14.98 The WA Government believes that this Working Party would be an effective tool to support the cultural change required in schools to reduce the effects of cyber-bullying.[88]

14.99 The WA Education Department, the WA Catholic Education Office and the Australian Independent Schools (WA) have a close relationship with ACMA, ensuring that all their schools have access to material that it has developed.

14.100 The K-10 Syllabus embedded the national *Statement of Learning for Information and Communication Technologies* which included building an understanding of the legal, ethical and health and safety implications of using the online environment, and responsibilities as users and developers.[89]

14.101 A range of evidence-based intervention plans has been developed by the Child Health Promotion Research Centre to deal with bullying, compatible with Australian curriculums, programs and practice. As these represent best practice, the WA Government believes that they should be considered for wider implementation in Australian schools.[90]

14.102 Commissioned by the Department of Broadband, Communications and the Digital Economy, in 2009 the Child Health Promotion Research Centre conducted a review of cyber-safety literature. This provided the most recent and comprehensive review of cyber-safety issues conducted to date in Australia, including best practice safeguards.

Tasmania

Education

14.103 The Tasmanian Department of Education uses information and communications technology as a core skill across all areas of the curriculum. Each school develops a plan for their requirements, with a view to engaging the local community so that it is clear that responsible use of technology happens across a day, not simply during school hours. Within a safe and secure framework, schools have considerable freedom

88 Western Australian Government, *Submission 118*, pp. 4-5.

89 Western Australian Government, *Submission 118*, p. 5.

90 Western Australian Government, *Submission 118*, p. 6.

about their technology arrangements, as well as how they handle difficult issues.[91]

14.104 Parents/carers, students and teachers must all sign 'conditions of use' forms, and information sessions are organised to educate them about cyber-safety, these are not mandatory for parents/carers. However, it appears that '95-plus percent' of parents/carers sign and return these agreements, and use is made of any opportunities that arise for teachers/principals to complete the process.[92]

14.105 The Department uses a filtering service provided by Telstra Corporation that allows sites to be blocked routinely, as well as individual URLs. While Web 2.0 technologies such as YouTube and Facebook are allowed into schools by default, primary students are not allowed to access Facebook because of age restrictions. A high school can decide to block Facebook but, as the aim is to educate students in the responsible use of technology, a teacher may construct a lesson using Facebook.[93]

14.106 Detailed reports are kept on a range of incidents at schools, and information is therefore available on students' use of technology. Strategies are also in place within schools to support students after events that occur on social networking sites.

14.107 A Memorandum of Understanding has been reached with the Tasmanian Police because of concerns about the number of violent incidents being filmed on mobile phones. In operation in part of the State for two years, it is likely to be extended to the rest of Tasmania later in 2011.[94]

14.108 When there has been a violent incident at a school, the police are notified, their processes are followed and they decide whether to take action on behalf of the Department. The police can also be involved in approaching, for example, YouTube through the AFP to remove unsavoury material.[95]

---

91 Mr Trevor Hill, Director, Information Technology Services, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS4.

92 Mr Trevor Hill, Director, Information Technology Services, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS4.

93 Mr Trevor Hill, Director, Information Technology Services, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, pp. CS5-6.

94 Ms Liz Banks, Acting Deputy Secretary, Early Years and Schools, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, pp. CS7-8.

95 Ms Liz Banks, Acting Deputy Secretary, Early Years and Schools, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. 8.

14.109 While teachers have to apply periodically for re-registration, unless they have been outside the profession for some time, there is no requirement for 'refresher' professional courses.[96]

14.110 While Departmental schools are able to use ACMA's Help Button but, because they can decide how they use it, the rate of introduction has not been high.[97]

Northern Territory

Education

14.111 The Northern Territory Government considered that governments had an important role in developing policies and programs to prevent and deal with all forms of bullying, including cyber-bullying. They also ensured that schools are appropriately supported and resourced to provide parents/carers and teachers with access to training about cyber-bullying and other online safety issues.

14.112 Schools in the Northern Territory therefore, have policies, aligned to the *Safe Schools Northern Territory Code of Behaviour.* Parents/carers and students are required to sign an 'Acceptable Use' agreement covering in general terms the inappropriate use of the online environment, including bullying and harassment.[98]

14.113 Positive Behaviour Advisors in schools also taught Student Representative Councils and School Captains, of public, Catholic and independent schools, about dealing with cyber-bullying with the expectation that they will share this approach with their schools.

14.114 The Territory's Education Department is developing a professional Learning on Demand Module in cyber-safety for its educators to undertake in 2011. It includes information on cyber-bullying, online reputations and cyber-stalking.[99]

14.115 While the sample size of cyber-bullying incidents in the Territory is insufficient to provide objective analysis, incidents have increased as young people gain greater online access.

---

96 Ms Liz Banks, Acting Deputy Secretary, Early Years and Schools, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS12.

97 Mr Trevor Hill, Director, Information Technology Services, Department of Education Tasmania, *Transcript of Evidence*, 20 April 2011, p. CS13.

98 Northern Territory Government, *Submission 84*, p. 7.

99 Northern Territory Government, *Submission 84*, p. 7.

14.116 School based police officers in the Territory have a significant role in the investigation of cyber-bullying complaints, and the delivery of safety instruction to young adults. They have been delivering education awareness presentations since 2008.[100]

14.117 These have been complemented by the immediate and thorough investigation of all complaints about cyber-bullying within the school environment, including requirements for parental/carer support and information on the consequences of misuse of carriage services. Education and encouragement is also provided to parents/carers and families to become more conversant with the online environment, and to monitor actively what young people are accessing on the Internet.

The Australian Capital Territory

14.118 The ACT Government acknowledged the need to take advantage of opportunities presented by developments in the online environment, while recognising the need to educate and protect young people against associated risks. This environment provided a means for citizens to have access to information that was consistent with the *Human Rights Act 2004* (ACT). It contained provisions about protecting families and children, freedom of expression and taking part in public life.[101]

14.119 The ACT is actively involved in combating cyber-crime and cyber-safety, both within the Territory and through cooperation with other jurisdictions. Agencies have introduced programs to educate young people on the safe use of the online environment, and to equip those in responsible positions with the skills to address issues that may arise.

14.120 The *Children and Young People Act 2008* (ACT) provides for the promotion, wellbeing, care and protection of young people in ways that recognises their right to grow in a safe and stable environment.[102] Under the *National Framework for Protecting Australia's Children*, initiatives are under way, including:

- The *ACT Young People's Plan 2009-2014* took account of issues of importance to young people, including measures to be taken to address cyber-bullying, and
- The ACT Children and Young People's Commissioner is obtaining the views of children and young people on issues including the use

100 Northern Territory Government, *Submission 84*, p. 6.

101 ACT Government, *Submission 82*, p. 1.

102 ACT Government, *Submission 82*, p. 2.

> of online media tools. The Commissioner will then advise the Government on how to improve services for this group.[103]

14.121 Commenting on programs in the ACT, the Australian Education Union noted that:

> there is a Safe Schools Taskforce which is a cross-sectoral group with representation from each school sector, the Youth Advisory Council, parent groups, principals, education unions and ACT Policing. The taskforce examines policies and procedures and makes recommendations to maintain and improve the safety of children and young people in ACT schools. These recommendations have resulted in new or updated policies (including Providing Safe Schools P-12, Countering Bullying, Harassment and Violence in ACT Public Schools, the Keeping Children Safe in Cyberspace guide and the Code of Conduct for public schools, outlining what is expected of all people when on ACT public school grounds), plus associated pamphlets and posters for schools and families. The taskforce is currently planning a forum for students on cyber-safety in 2011.[104]

Education

14.122 The Government believed that the ACT is at the forefront of information and communications technology. It has used the *myclasses* Virtual Learning Entertainment Environment since 2003. At the beginning of a school year, or on enrolment, all students must sign an 'Acceptable Use' form before they can go online. They are monitored while online, and inappropriate websites are blocked on the school system.[105]

14.123 In 2009, a blogging feature for teachers was introduced into the *myclasses* environment. When it was apparent that some students were using it inappropriately, and without teachers' knowledge, it was removed.

14.124 A new Virtual Learning Entertainment Environment, Connected Learning Communities, has been deployed to all ACT public schools to replace *myclasses*. It enables schools to access digital content to enrich programs via the Internet. During its selection and development, consideration was given to the level of risk and cyber-safety concerns that it could bring.[106]

---

103 ACT Government, *Submission 82*, p. 2.

104 Australian Education Union, *Submission 11*, p. 10.

105 ACT Government, *Submission 82*, pp. 3-4.

106 ACT Government, *Submission 82*, p. 4.

14.125 The Connected Learning Communities provides teachers with the opportunity actively to develop essential skills and capabilities in students to participate safely in the online environment. Its features include:

- An ACT Safe-Report Abuse button located at the top of every page. This would automatically open a new mail message in which students can type in the issue. The recipient of these messages would be a selected staff member;
- The individual user name and password given to each student, which must be authenticated before access is given to the network, and prevents students from making anonymous contributions within this environment;
- Students and teachers will be able to use a range of social networking tools that were once unavailable in classrooms because of privacy issues, and the risks of students engaging online with unknown people. Schools will be able to select the people with whom their students connect: their year, the whole school or across schools; and
- If students are using the networks inappropriately, monitoring and tracking systems will allow schools to lock accounts within seconds and examine the students' digital footprint.[107]

14.126 The ACT works with other organisations, including the AFP, ACMA and the *Budd:e* Program, to educate teachers, parents/carers and students about Cyber-safety. This included the distribution of posters brochures and teaching materials to schools. Many schools had hosted information nights about safety online and cyber-bullying, and those which had taken part had indicated that these were well-received and 'extremely beneficial'.[108]

14.127 While reports of specific incidents are low in the ACT, where cyber use escalated into bullying behaviour in a school, it is important that schools respond appropriately. These incidents are dealt with under a range of policy documents developed in accordance with the National Safe Schools Framework. ACT policies will be updated to reflect changes that are required in the recent review of the Framework.[109]

14.128 A Safe Schools Taskforce has been created to ensure that the ACT remains a national leader in tackling bullying at school, and that all ACT schools

107 ACT Government, *Submission 82*, p. 5.

108 ACT Government, *Submission 82*, pp. 5-6.

109 ACT Government, *Submission 82*, p. 6.

deal with it in the same manner. Including systemic Catholic and independent schools ensures that the best ideas from the three sectors are shared and used for the benefit of all students.

14.129 In 2010, a sub-group of this Taskforce was formed specifically to consider cyber-safety and cyber-bullying issues.[110] A forum, involving Year 9 students from all ACT schools, teachers, parents/carers and organisations such as the AFP, was held in Canberra on 18 March 2011.

Non-government and industry responses

14.130 Australian organisations and service providers have taken a range of measures to encourage cyber-safety, and to combat cyber-bullying in particular. The following individuals and organisations that participated in the Inquiry have devised a range of programs dedicated to dealing with the abuse, and to improve cyber-safety for young people generally.

Australian organisations

14.131 The Safer Internet Group includes organisations such as the Australian Council of State School Organisations , the Australian Library and Information Association, Google, iiNet, the Inspire Foundation, the Internet Industry Association, the Internet Society of Australia, Internode, the System Administrators Guild of Australia and Yahoo!.[111] The Group aims to develop 'the Internet as a platform for education, communication and economic activity and acknowledges that for the vast majority of users, the internet is a safe place' and:

> advocates for effective action to be taken to ensure that Internet users, and particularly children, have a safe experience online, while preserving the benefits of open Internet access for all Australians. The SIG believe that the most effective way to protect Australia's children on the Internet is achieved by a combination of safety enhancing measures which include a primary focus on effective education and comprehensive policing of the Internet.[112]

14.132 The Stride Foundation is a not-for-profit organisation dedicated to helping improve the physical, mental and social well-being of young people and

110 ACT Government, *Submission 82*, p. 7.

111 Safer Internet Group, *Submission 12*, p. 1.

112 Inspire Foundation, *Submission 3*, p. 11.

their communities. Its purpose is to empower young people to realise their full potential, and to have the opportunity for brighter futures. It started as a peer-support foundation, and now takes on the cultural change of schools. It is not the same as other organisations with similar aims because it works with young people before any issues encountered, such as bullying, conflict, stress, depression suicide or low self-esteem, begin to have negative effects on lives.[113]

14.133 The keys to Stride's *CyberS@vvy* program are:

- Understanding the lack of empathy involved;
- Looking at how digital footprints work, and how students and perpetrators can be traced;
- Legal penalties; and
- How to refer serious issues to a trusted adult.[114]

14.134 Berry Street is the largest independent, not-for-profit child and family welfare organisation in Victoria, providing an extensive range of services for young people and families across the State.[115]

14.135 It approached cyber-safety through vulnerable young people living out-of-home and engaged in alternative education. One of its aims is to increase online access for those young people. As has been pointed out, those in out-of-home care can have less access to technology than their peers. This organisation sees technology as a valuable tool for connecting socially isolated young people with their community, and with their families.[116]

14.136 With funding from Telstra Corporation, the Victorian Office of the Child Safety Commissioner and the State's Department of Human Services, Berry Street developed *BeNetWise* in 2009. Its key aims related to raising awareness about technology, the value of technology for this group and the importance of online safety for such vulnerable young people.[117]

---

113 Stride Foundation: *Submission 6*, p. 1; Ms Kelly Vennus, Programs and Training Manager, *Transcript of Evidence*, 9 December 2010, p. CS2.

114 Ms Kelly Vennus, Programs and Training Manager, Stride Foundation, *Transcript of Evidence*, 9 December 2010, p. CS3.

115 Berry Street, *Submission 95*, p. 2.

116 Ms Sherree Limbrick, Director, Statewide Programs, Berry Street, *Transcript of Evidence*, 9 December 2010, pp. CS3-4.

117 Berry Street: *Submission 95*, p. 5; Ms Sherree Limbrick, Director, Statewide Programs, *Transcript of Evidence*, 9 December 2010, p. CS3.

14.137 The Alannah and Madeline Foundation included cyber-bullying within its *eSmart Schools Framework* which provided a 'consistent and practical' whole-school approach for the implementation of evidence-based cyber-safety programs and practices. Because it needed to be addressed head-on, *eSmart* was not another program for cyber-safety, but a system for driving its implementation in schools. It was a road map or model for cultural and behaviour change targeting the whole school community, not a one-off lesson, unit of work, program or policy isolated from the day-to-day business of schools.[118]

14.138 The National Association for the Prevention of Child Abuse and Neglect has a range of programs and campaigns that educate children and young people in their online environments. They can be used, or adapted for use, in other jurisdictions, and include:

- *SOSO*, a digital collaboration with the digital marketing group Zuni; and
- Cyber Bullying Affects Real Lives, of which *Web Warriors* is a key element that asks young people to take a stand against cyber-bullying.[119]

14.139 The Inspire Foundation was established in 1996 as a direct response to Australia's then escalating rates of youth suicide, seeking to have a 'global impact' on the mental health and well-being of young people. It serves those aged between 14 and 25 through three national programs.

14.140 They are at the centre of all the Foundation does: as partners in the development and delivery of all its initiatives. It uses technology innovatively to reach young people and to build trusted social brands that are a part of their landscape. Its work is evidence-based and underpinned by research and evaluation conducted in partnership with academic institutions and research centres.[120]

14.141 To deal with threats to cyber-safety, and cyber-bullying in particular, it recommended a multi-faceted, cross sectoral and educative approach. This view was based on evidence and experience that restrictive approaches to technology are ineffective.[121]

---

118 Alannah and Madeline Foundation: *Submission 22*, p. 35; Dr Judith Slocombe, Chief Executive Officer, *Transcript of Evidence*, 11 June 2010, p. CS7.

119 National Association for the Prevention of Child Abuse and Neglect, *Submission 97*, p. 3.

120 Inspire Foundation, *Submission* 3, p. 1.

121 Inspire Foundation, *Submission* 3, p. 6.

14.142 The Alannah and Madeline Foundation believes that *eSmart* is not just another cyber-safety program, but a system for driving its implementation in schools as part of a planned and systematic approach. It provides a consistent and practical whole-school approach for the implementation of evidence-informed cyber-safety programs and practices. It is a culture and behaviour change model targeted at the whole school community and, as such, is not a one-off lesson, unit of work, program or policy that sits in isolation from the day-to-day business of schools. [122]

14.143 More specifically, *eSmart* aims to:

- Integrate cyber-safety with schools' current knowledge and practices about well-being, including policies such as the NSSF;
- Assist schools to develop more effective curriculum around cyber-safety and wellbeing and the smart use of technologies;
- Help give teachers skills in smart, safe and responsible use of technologies;
- Assist school communities in developing safe and supportive schools where bullying and violence are minimised and the values of responsibility, resourcefulness, relationships and respect are fostered in cyber-space; and
- Assist schools in becoming cyber-safe.

14.144 *eSmart* supports exploration of:

- Protective behaviours;
- Supportive and relationship building behaviours, and
- Reporting incidents.

14.145 It embraces:

- Whole-of-school well-being issues including values/relationships/self-esteem;
- E-security;
- Ethics including downloading and plagiarism, and
- Criminal activity, including sexual harassment and predation.

122 Dr Judith Slocombe, Chief Executive Officer, Alannah and Madeline Foundation, *Transcript of Evidence*, 11 June 2010, p. CS7.

14.146 *eSmart* is underpinned by the positive embrace of information and communications technology and the promotion of smart use of technology. It is designed to:

- Help schools develop policies and practices (developed with input from students and parents) encouraging students to use technology responsibly and respectfully;
- Point schools to high quality teaching resources on cyber-safety and those which help create a safe, respectful and caring environment;
- Encourage schools to embrace the positives of Internet and communications technology within their teaching practice to enhance learning;
- Establish a system for schools to provide evidence that they are actively implementing these policies and practices, and
- Help reduce the digital divide between adults and young people, so adults can become a credible source of advice on avoiding the risks of cyber-space.

14.147 The major mechanism for delivery of *eSmart* into schools is an interactive website. Schools are further supported by other resources such as a welcome kit, newsletters and a Help Desk, as well as training in using the system.[123]

14.148 Roar Educate applauded the *eSmart* initiative, as a key to both awareness and cultural change within schools. It did not believe however that, in isolation, it can bring about the holistic approach needed by schools to manage cyber-safe risk management. *eSmart* needs to be complemented by other systems.[124]

Aboriginal initiatives

14.149 Dr Julian Dooley, commented that

> In 2006 we began a project to reduce cyberbullying behaviour experienced by Aboriginal children in the mid-west of Murchison region of Western Australia. Aboriginal community members, including elders, children, young people, parents, carers and Aboriginal school staff, talked with us about what they called 'bullying', why they think it happens and how it feels to be

123 Alannah and Madeline Foundation, *Submission 22*, pp. 35-36.

124 Mr Craig Dow Sainter, Managing Director, Roar Educate, *Transcript of Evidence*, 20 April 2011, p. CS17.

> Aboriginal and be bullied. This project led to the development of a number of important outcomes, including a website www.solidkids.net.au which provides evidence based and culturally appropriate information on strategies for young Aboriginal people, schools and families. [125]

14.150 Although these are very important resources, much more work is needed to protect Aboriginal youth.[126]

Australian ICT industry bodies

14.151 Since 2002, Australian Internet service providers compliant with Internet Industry Association Codes have been eligible to apply for 'IIA Family Friendly ISP' status. These Codes exist as part of Australia's co-regulatory regime, and they are legally enforceable by ACMA. Such Internet service providers are authorised to display a logo which signifies adherence to best practice standards. The Association noted that ISPs representing about 85 percent of the market are family friendly.

14.152 Under the registered Code, Internet service providers providing access to users within Australia are required to:

- Take reasonable steps to ensure that Internet access accounts are not provided to persons under the age of 18 years without the consent of a parent, teacher or other responsible adult. A number of suggested options for achieving this are included in the Code;
- Take reasonable steps to encourage commercial content providers to use appropriate labelling systems, and to inform them of their legal responsibilities in regard to the content they publish. The Internet Industry Association has compiled a resource for this purpose, and Internet service providers are advised to direct users to the Association's URL;
- Provide an optional filter or filtered service to users on a cost recovery basis, and
- Take reasonable steps to provide users with information about:
  - ⇒ supervising and controlling children's access to Internet content;
  - ⇒ procedures which parents can implement to control children's access to Internet content;
  - ⇒ their right to make complaints to ACMA about online content; and

125 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS5.

126 Dr Julian Dooley, *Transcript of Evidence*, 11 June 2010, p. CS5.

⇒ procedures by which such complaints can be made.[127]

14.153 The Association referred to the 'very specific parameters' around the sites that are subject to ACMA's take-down provisions. These fall into the 'prohibited content' classification under the Codes underpinned by legislation. Such sites are required to be removed by 6pm on the business day following the day on which they are notified. When sites are subject to take-down, they are subject to limits of Australian jurisdiction. The 'vast majority' of such sites are not hosted here.[128]

14.154 Google Australia works closely with a network of experts who advise it on promotion of child safety and how to combat abuse in its products. It drew attention to the range of measures that it takes to do these things, including the advice that it provides to its users.[129]

14.155 Microsoft Australia believed that the following responses would assist parents/carers to deal with cyber-bullying:

- Communicate by discussing the issue with children, and encourage them to report it to a trusted adult;
- Block communications through filters, and children not to respond to the abuse;
- Investigate so that they know what children are talking about, and what they do online;
- Use Family Safety Software which can supply an activity report on computer usage. This in turn can be a starting point for a discussion about online activities; and
- Report by knowing who to contact if a young people is being cyber-bullied, such as her/his school, the site service provider, and the police.[130]

14.156 Microsoft Australia also commented on its recently established Digital Crimes Unit, which includes:

> A worldwide team of lawyers, investigators, technical analysts and other specialists whose mission is to make the Internet safer

127 Mr Peter Coroneos, Chief Executive Officer, Internet Industry Association, *Transcript of Evidence*, 11 June 2010, p. CS10; Internet Industry Association, *Submission 88*, p. 13.

128 Mr Peter Coroneos, Chief Executive Officer, Internet Industry Association, *Transcript of Evidence*, 11 June 2010, pp. CS16-17.

129 Google Australia & New Zealand, *Submission 13*, p. 2,

130 Microsoft Australia, *Submission 87*, p. 3.

through strong enforcement, global partnerships, public policy and technology solutions.[131]

14.157 Yahoo!7 referred to the 'distinct lack' of evidence into how Australian young people engage with the online environment, and how their parents/carers see the risks of using the Internet.

14.158 It also believed that further research into the prevalence and scale of online safety risks would inform and shape the debate about which safety measures would be most effective in managing those risks.[132]

14.159 Yahoo!7 provides training to the law enforcement community and has created the Australian Law Enforcement Process Guide.

14.160 It has also:

- a dedicated online safety education site called Yahoo!7 Safely with information for parents of younger children and teenagers about how to be safe online;
- been an active member of the Consultative Working Group on Cybersafety and the Safer Internet Group;
- been an active supporter of Safer Internet Day for two consecutive years;
- been working closely with the Australian Competition and Consumer Commission on their Scamwatch and consumer fraud efforts; and
- through the Internet Industry Association, developed a family friendly filtering accreditation which can be used by Internet service providers and filtering software vendors, and is developing a voluntary code whereby providers would actively filter websites containing child abuse images out of their services.[133]

14.161 It gave examples of its initiatives, in education, policing, safer social networking, research and technology, to improve safety online. It noted that Yahoo! has enabled a SafeSearch feature within Yahoo!7 to prevent the display of adult content in queries. Parents/carers can lock this function on, and young people registered as under 17 years old cannot turn it off.[134]

---

131 Microsoft Australia, *Submission 87*, p. 2.

132 Yahoo!7, *Submission* 2, pp. 2-4.

133 Yahoo!7 *Submission 2.2*, pp. 1-2.

134 Yahoo!7, *Submission 2*, pp. 3-4.

14.162 Yahoo!7 works closely with Australian law enforcement agencies to provide assistance when its services are abused. This included establishment of a 24 hour/seven days per week compliance function which can respond immediately if Yahoo!7 is contacted about a situation indicating that a young person may be in danger.[135]

14.163 Telstra Corporation is an industry partner with the Australian Government to link young people, parents and teachers with expert cyber-safety advice and targeted information via ACMA's Cybersmart website. It has agreed to cross-promote the Authority's website as part of its focus on helping to protect Australians from cyber-bullying and invasions of privacy.[136]

14.164 Other activities by Telstra include:

- participation on the Consultative Working Group on Cybersafety ;
- providing tools, tips and educational information to customers;
- supporting Safer Internet Day, the Australasian Consumer Fraud Taskforce's Fraud Week, Privacy Week and National Cyber- Security Awareness Week;
- its Computer Emergency Response Team;
- being an original partner of the Virtual Global Taskforce;
- being a dedicated Trading Post Trust and Safety team; and
- tasking a company Chief Privacy Officer and Privacy Managers to ensure that business units adhere to its privacy policies and procedures.[137]

14.165 Singtel Optus noted that the Australian Mobile Telecommunication Association has developed a range of fact sheets and other material for parents and young people on topics such as bullying and mobile phones. There is also a website that provides information on bullying and online safety generally.[138]

14.166 Netbox Blue is a privately owned Internet management company, providing schools, businesses and government organisations with tools to

135 Yahho!7, *Submission 2*, p. 3.

136 Telstra Corporation, *Submission 14*, p. 7.

137 Telstra, *Submission 14*, p. 5.

138 Singtel Optus, *Submission 42*, p. 2.

protect their networks from internal/external threats, control data threats and ensure staff/students use the Internet safely and productively.[139]

14.167 It has devoted more than three years to develop 'patent-pending and unique' technology to address issues in the Inquiry's Terms of Reference, including cyber-bullying. It believed that this software would prevent inappropriate communications on social networking sites such as Facebook and Twitter. It could be used at schools, on laptops provided for use outside those networks and soon, at homes. It noted that this technology was already being used at schools across Australia.[140]

14.168 Device Connections is the exclusive distributor of My Mobile Watchdog, 'a sophisticated safety technology' that allows parents to see:

- the full content of text messages received and sent;
- photos received and sent;
- the full contents of emails received and sent, and
- a log of the mobile phone calls received and made, their time and duration.

14.169 This technology is aimed at children aged from six to 14, and was established to help parents educate and manage their children's safety. It was driven by concerns about cyber-bullying and sexting. Parents can set up an alert notification function within the system so that, when a suspicious or unauthorised person tries to call, text or email a young person, the communication is routed through the My Mobile Watchdog data centre. Notifications or alerts by SMS message or email are sent 'instantly' to all the people nominated in the parents' web account.[141]

14.170 My Mobile Watchdog can be used on all phones operating on Windows Mobile 5 and 6, it was recently launched for all android operating systems and the capability is being developed for more handsets. Device Connections sees this system as 'only one piece' in a very complex puzzle of managing cyber-safety education and training for parents/carers, the community and young people themselves. This service costs about $150 per year, providing licences for up to five children.[142]

---

139 Netbox Blue, *Submission 17*, p. 1.

140 Netbox Blue, *Submission 17*, pp. 2-3.

141 Device Connections: *Submission 51*, p. 3; Mr Geoffrey Sondergeld, Director, *Transcript of Evidence*, 17 March 2011, p. CS48.

142 Mr Geoffrey Sondergeld, Director, Device Connections, *Transcript of Evidence*, 17 March 2011, pp. CS49-51.

14.171 It included in its submission a report from the United States about the effectiveness of My Mobile Watchdog in helping 'parents monitor and keep their children safer' while using their mobile phones.[143]

14.172 The Communication Alliance Industry Code deals with the *Handling of Life Threatening and Unwelcome Communications*, and is an example of co-regulation.[144]

Marketing

14.173 The Australian Direct Marketing Association is the peak industry body for the Australian direct marketing industry and operates a Direct Marketing Code of Practice which includes specific provisions to address marketing to minors.[145] The Code specifies that members limit the sale of restricted goods and services to minors and indicate when parental consent is required. The Australian Direct Marketing Association has a number of platforms designed to provide guidance to its members about appropriate conduct when interacting with young people.[146]

143 Device Connections, *Submission 51*, p. 22.

144 Australian Communications Consumer Action Network, *Submission 1*, p. 5.

145 Australian Direct Marketing Association, *Submission 36*, pp. 3-4.

146 Australian Direct Marketing Association, *Submission 36*, p. 4.