SUBMISSION No. 80

Australian Government | acma

Australian Communications and Media Authority

Joint Select Committee on Cyber-safety
Submission

JULY 2010

Overview

The Australian Communications and Media Authority (ACMA) welcomes the opportunity to make this submission to the Joint Select Committee on Cyber-Safety (the Committee) in relation to the inquiry into the safety of children and young people on the internet.

The Committee's inquiry comes at an exciting time in Australia's transformation to a Digital Economy. The internet has brought tremendous benefits to Australians in sharing information, keeping in touch, working and play.

However, behaviours of people online may present risks to others, particularly the more vulnerable, including children. The management of online risk at a time when online social (and financial) transactions have become relatively routine is a key focus for the ACMA.

The ACMA has been operating in the cybersafety space for more than ten years. Its remit stems from the Online Content Scheme included the *Broadcasting Services Act 1992*. Under the Online Content Scheme, the ACMA's role is to:

- Investigate complaints about prohibited and potentially prohibited online content—the ACMA has undertaken more than 10,000 investigations into online content under the scheme; and
- Facilitate a system of co-regulation where the internet industry developed codes of practice which were registered by the ACMA.

The ACMA's regulatory role in relation to online content is certainly not the only role it undertakes in helping Australians to address risks online. Increasingly, a large part of the ACMA's role in terms of our resources and activity is in delivering on a broad range of cybersafety, education and awareness programs. This role has evolved over time.

Most recently, in 2009-10, the ACMA received an additional $21 million over five years as part of the government's cybersafety plan. These funds support a comprehensive range of information and resources designed to meet the needs of children, parents, carers, teachers and library staff.

Under the Cybersmart brand, the ACMA delivers a diverse, comprehensive and effective suite of programs and resources tailored to meet the needs of teachers, librarians, parents, children and teens today.

The ACMA has focussed its submission on these resources and how these, and research that underpins them, is relevant to the Committee's Terms of Reference.

Cybersmart programs are in strong demand across Australia and have proven extremely popular. Since 2009 there has been:

- 131,902 attendees at over 1,300 Internet Safety Awareness Presentations;
- 5,153 attendees at over 200 Cybersmart Professional Development for Educators events;
- 260,000 unique visitors to the ACMA's Cybersmart website;
- 11,500 students participating in a Cybersmart Detectives event at more than 400 schools; and
- 1.5 million Cybersmart brochures distributed across Australia.

A summary of the ACMA's Cybersmart programs is at Attachment A.

The ACMA works collaboratively with industry, other levels of government and the non-government sector in Australia on the development and delivery of its programs. It also works with international partners to ensure that it is delivering world class and world first product which is tailored and relevant to the Australian environment.

As an evidence-based regulator, the ACMA also ensures that its programs are based on solid research—tapping into the best from Australian and international researchers as well as commissioning tailored research where needed.

For example, the ACMA refers the Committee to the reports of its three-year program of research examining developments in safety initiatives around the world aimed at protecting both minors and adults who access content on the internet. The framework identified in its 2008 report has been used by the ACMA for considering specific online risks and a range of mitigation strategies. The report notes that majority of measures that are used to mitigate online risk are only relevant for one or two types of risk category (see pages 10-11).

In 2010-11, the ACMA will be delivering further cybersafety initiatives including:

- From July 2010, new Cybersmart Parent resources will be launched in hard copy and online. These resources are based on the ACMA's research into the information needs of parents, including the areas parents are most concerned about, and the delivery channels that work best for them.
- An innovative interactive e-learning platform is under development to give teachers and schools more flexibility in accessing the ACMA's very successful Outreach program. This initiative will not only assist in better meeting school and teacher demand for cybersafety information but will also be accessible by teachers (including casual relief teachers) in regional and remote areas of Australia.
- A Pre-Service Teacher training program will be rolled out to universities across Australia. This program is built on the successful face-to-face Professional Development for Educators workshops. This new program will equip final year student teachers with the skills, knowledge and classroom resources to help their future students stay safe online.
- A new DVD for teenagers dealing with online privacy will be developed for launch in 2011.
- The ACMA's cybersafety resources and information are soon to be made available in multiple languages to meet the information needs of non-English speaking Australians.
- The ACMA is finalising a research study into the cybersafety needs of young people with learning difficulties and is involved in a working group looking at the cybersafety needs of vulnerable or disadvantaged youth. This work will inform the development of resources to target these audiences.

The ACMA will also continue to work with the Department of Broadband, Communications and the Digital Economy and the Consultative Working Group on Cybersafety on projects such as the common cybersafety help button, which will provide ready access to online help through a common interface.

The ACMA considers that it is well placed to assist the Committee in its deliberations on this important subject. It would welcome further opportunities to brief the Committee on its research and its programs.

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

The ACMA would recommend to the Committee a number of recent Australian and international research reports which provide information and analysis of issues relevant to this term of reference.

Key physical points of access

The *Children's Participation*[1] survey conducted by the Australian Bureau of Statistics in 2009 indicated that a higher proportion of children used the internet at home (92%) than at school (86%). At the time of this survey only 4% of children used a mobile phone to access the internet.

Since 2000, the ACMA has undertaken a sequence of research projects exploring children's use of online technologies with a focus on the home environment. These include:

- *Internet@home* (2001);
- *kidsonline@home* (2005);
- *Digital Media in Australian Homes (2006)*
- *Media and Communications in Australian Families* (2007), followed by a series of short reports (2009); and
- *Click and Connect* (2009)

The research indicates that Australian children access the internet through a diverse range of delivery mechanisms. These include:

- Computers (desktop, laptop, netbook)
- Mobile phones – data published by the ABS from its *Children's Participation* survey indicates that 31% of children aged 5-14 years had exclusive use of a mobile phone
- Gaming devices (such as Nintendo DS, Wii, PSP, PS2 and PS3)

The ACMA's survey *Media and Communications in Australian Families*[2] indicated 'first use' at about age 5, but there is anecdotal evidence that children are going online at younger and younger ages.

The ACMA's *Click and Connect*[3] research found that as children age they spend more time online:

- Children aged 8 to 9 years use the internet for an average of 1 hour, 6 mins every two days.
- Young people aged 16 to 17 years average 3 hours, 30 mins on the internet every day.
- Younger children are more interested in individual activities online, such as playing games—83 per cent of 8 to 11 year-olds reported online gaming as the most popular use of the internet.

[1] *Children's Participation in Cultural and Leisure Activities*, Australian Bureau of Statistics, October 2009
[2] *Media and Communications in Australian Families*, Australian Communications and Media Authority, December 2007
[3] *Click and Connect: Young Australians' use of online social media*, Australian Communications and Media Authority, July 2009

- By comparison, young people aged 12 to 17 use the internet mainly for social interaction—81 per cent of 12 to 17 year olds nominated social networking services as their main reason for going online.

In addition, the research demonstrated a high level of use of social networking services:

- Young people, aged 12 to 17, have a very high level of use of social networking services. Approximately 97 per cent of 16 to 17 year olds surveyed reported using at least one of these services, compared to 51 per cent of children aged 8 to 11 years.
- Fifty four per cent of 12 to 17 year olds claim that 'chatting to friends from school' is their main reason for using social networking services. The *Children's Participation* survey indicated that younger children used the phone primarily to contact family rather than friends.
- By comparison, only 17 per cent of 12 to 17 year olds claim to use the internet to 'make new friends'.

Young people's awareness of risk

Click and Connect also demonstrated that children and young people have a high awareness of cybersafety risks, and identify activities such as 'posting personal information' as high risk behaviour.

Despite this, some young people deliberately engage in risky behaviours, and the tendency to do this rises with age. Of those aged 16 to 17 years:

- Sixty-one per cent report accepting 'friend requests' from people they don't know offline.
- Seventy-eight per cent claim to have personal information, such as a photograph of themselves, on their social networking profile pages, compared to 48 per cent of 8 to 9 year olds.
- 17 per cent of 12-17s claim that one of their top three reasons for using social networking services is to 'make new friends'.
- Conversely, use of privacy settings on profile pages appears to be greater amongst the older age groups.

The ACMA has conducted a three-year program of research examining developments in safety initiatives around the world aimed at protecting both minors and adults who access content on the internet. These reports have helped shape the ACMA's Cybersmart programs and are discussed further under term of reference (iii).

The ACMA also refers the Committee to the findings of research conducted by other agencies within Australia and overseas that have shaped the development of the ACMA's cybersafety programs including:

- Dooley, JJ; Cross, D; Hearn, L; Treyvaud, R, *Review of existing Australian and International Cyber-safety Research* Child Health Promotion Research Centre, Edith Cowan University, Perth, May 2009
- Lenhart, A; Madden, M *Teens, privacy and online social networks* PEW Internet and American Life Project, 2007
- Rideout, VJ; Foehr, UG; Roberts, DF *Generation M²: Media in the Lives of 8 to 18-year-olds*, Kaiser Family Foundation, Menlo Park, January 2010
- Livingstone, S; Haddon, H (editors), *kids online: opportunities and risks for children*, Policy Press UK, 2009 (incorporating papers and discussions generated as part of the EU Kids Online project)

- Byron, T. (2008) *Safer Children in a Digital World: The Report of the Byron Review:* (http://www.dcsf.gov.uk/byronreview/)
- Cross, D., Shaw, T., Hearn, L., Epstein, M., Monks, H., Lester, L., & Thomas, L. (2009). *Australian Covert Bullying Prevalence Study (ACBPS)*. Child Health Promotion Research Centre, Edith Cowan University, Perth. (http://www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/research.aspx)

ACMA programs are identified at Attachment A. In addition to our research activities, programs most relevant to this term of reference are:

- The Cybersmart website and the suite of education resources for young people and teachers contained on the 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.

TOR(ii) the nature, prevalence, implications of and level of risk associated with cyber-safety threats, such as:

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

There is an extensive range of national and international research on issues relevant to this term of reference.

The ACMA draws the Committee's attention to the research of Dr Peter Smith (University of London) which was presented to the e-Youth Conference in Belgium in May 2010. Dr Smith's presentation gave an overview of the current research on cyberbullying and identifies the challenges and opportunities for research in the area.

Key observations from this conference also illustrated the need for increased focus on *harm* as opposed to perceptions of *risk* in cybersafety programs (Professor Sonia Livingstone, London School of Economics). Online safety messaging has generally started from the assumption that any degree of risk is negative for the child, while emerging research suggests that a certain level of risk taking is necessary for the development of resilience amongst young people. This and related research findings will continue to be taken on-board by the ACMA as it reviews its cybersafety messaging and adapts its programs to reflect new understandings.

Research programs have also progressively been redesigned to incorporate the views and experiences of young people and children, with the findings indicating that issues such as cyberbullying are of increasing concern to them. Understanding how this group uses the internet, as well as perceptions of online risks is important to the ACMA when designing programs that are both relevant and effective in equipping young people, parents and teachers with the skills and knowledge necessary for safe and positive online experiences.

The ACMA's *Click and Connect* research sought to understand Australian young people's online content and contact experiences resulting from their participation in social media. The research found that young people aged 12 to 17 years using social networking services are more likely than eight to 11-year-olds to have received friend requests[4] from people they don't know (56 per cent compared to 35 per cent) and, as children age, they become far more likely to accept the request (23 per cent of eight to 11-year-olds compared to 61 per cent of 16 to 17-year-olds who had received a friend request had accepted a request). This is consistent with the increased acceptance of older teens to the use of social networking services as a good way to meet new people.

As their children age and begin to use social networking services more frequently, parents generally become aware that their children are interacting with people they don't know. 14 per cent of parents of 16 to 17-year-olds are aware their children meet online friends in person for example, compared with one per cent of parents of eight to nine-year-olds.

Similarly, as children age they are exposed to significantly more requests for personal details and other forms of contact such as webcams and Instant Messaging (IM) (at eight to nine years, only three per cent receive any requests for information or personal

[4] A 'friend request' refers to an unsolicited invitation from one social networking service user to another in order to be added to one and others social network or 'friends list'.

contact, which increases to 56 per cent by 16 to 17 years), although relatively few admit they provide the details or send the requests themselves (from one per cent of eight to nine-year-olds, up to 27 per cent of 16 to 17-year-olds).

Around one in three households (30 per cent) report having a webcam. Of those that do, older teenagers are far more commonly allowed to use it than younger members of the household. Eighty two per cent of 16 to 17-year-olds with a webcam are allowed to use it at home compared to 33 percent of eight to nine-year-olds.

Children and young people appear to be conservative with their use of webcams and generally only use them with relatives and friends they know in the real world. Overall, fewer than three per cent of children and young people aged eight to 17 have used a webcam with a stranger.

Cyberbullying

The ACMA's *Click and Connect* research sought to understand the extent to which children and young people had experienced cyberbullying, and had participated in cyberbullying themselves.

The research demonstrated that the incidence of cyberbullying increases with age. By the age of 16 to 17 years, nearly one in five (19 per cent) report having experienced some form of cyberbullying. In contrast, just one per cent of eight to nine-year-olds report having experienced cyberbullying. The largest increase in the incidence of cyberbullying occurs between the ages of eight to nine and 10 to 11, followed by a second smaller increase between the age groups of 10 to 11-year-olds and 12 to 13-year-olds.

The research also demonstrated that the overwhelming majority (98 per cent) of young people (12 to 17-year-olds) who had experienced a bullying incident reported taking some action in response. The most common action taken was to report the incident to a parent (mentioned by 72 per cent), followed by blocking the bully or messages (mentioned by 50 per cent).

When children and young people were asked if they had engaged in cyberbullying behaviour, less than 10 per cent admitted any involvement. The research indicates that older age groups were most likely to admit to cyberbullying.

Privacy

The ACMA's *Click and Connect* research found that while relatively few children and young people report having actively sent any personal details to people they hadn't met in person, many of those with a social networking page may be publicly displaying this information. It follows that if friend requests from unknown people are accepted, then they are able to view any content on a social networking service page. In the event that this page contains personal information, the 'new friends' will be able to access it.

Of those surveyed, children and young people who were social networking services users, were asked if they had posted any personal details (such as their mobile phone number, home address, full name, date of birth, a photo of themselves, or their school name) on their page. Only 22 per cent of 16 to 17-year-olds claim they have not put any of the details listed on their page, compared to 52 per cent of eight to nine-year-olds who claim they have not put any details on their page.

Generally the most common personal details to be posted on children and young people's social networking service pages are photos of themselves. Posting a photo of themself becomes more popular with age—by 16 to 17 years, two in three with a social networking service have posted a photo of themselves, compared to less than 25 per cent of eight to nine and 10 to 11-year-olds. Eight to nine-year-olds and 10 to 11-year-olds are more likely to report posting their date of birth than their photo.

Illegal and inappropriate content

Under the *Broadcasting Services Act 1992*, the ACMA has the regulatory responsibility for a hotline where Australian residents and businesses are able to make complaints to the ACMA about content they consider to be offensive and may be prohibited.

The ACMA has observed a steady increase in the number of complaints about online content it receives from the public, particularly complaints relating to overseas-hosted online child abuse and child sexual abuse material. Since 1 January 2000, the ACMA has investigated over 10,500 complaints about online content and taken action on over 8,000 items of prohibited content as a result.

In the period 1 July 2009 to 30 April 2010, the ACMA received 2,554 complaints, more than double the number of complaints received in the period 2008-09.

The ACMA must investigate all valid complaints and take action when it finds that content is prohibited. Under Schedule 7 to the Broadcasting Services Act, the following categories of content are prohibited content:[5]

- Any online content that is or is likely to be classified Refused Classification or X18+ by the Classification Board. This includes real depictions of actual sexual activity, depictions of bestiality, material containing excessive violence or sexual violence, detailed instruction in crime, violence or drug use, and/or material that advocates the doing of a terrorist act. It also includes child pornography, sometimes referred to as child sexual abuse material.
- Content that is or is likely to be classified R18+ and not subject to a restricted access system that prevents access by children. This includes depictions of simulated sexual activity, material containing strong, realistic violence and other material dealing with intense adult themes.
- Content that is or is likely to be classified MA15+, provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and that is not subject to a restricted access system. This includes material containing strong depictions of nudity, implied sexual activity, drug use or violence, very frequent or very strong coarse language, and other material that is strong in impact.

The increase in complaints received by the ACMA is likely to be due to a range of factors including:

- an increased number of Australian families who are online;
- greater awareness of the potential dangers of harmful content;
- increased awareness of how to report suspected prohibited content; and
- additional community interest in online content regulation issues and the role of the ACMA in this area.

The ACMA's website provides detailed information and a complaint form to assist people lodge complaints about online content (www.acma.gov.au/hotline). Complaints can also be submitted by email, post or fax.

Other relevant ACMA programs include the Cybersmart Online Helpline for young people who need in-depth assistance following a negative online experience. Further details are at Attachment A.

[5] The regulatory scheme is underpinned by the National Classification Scheme that applies to traditional media platforms including cinema, DVDs, computer games and publications. The National Classification Scheme requires assessment of material on the basis of the impact of classifiable elements such as sex, violence, nudity and drug use.

TOR(iii) Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) their effectiveness and costs to stakeholders, including business

The ACMA considers a multi-layered approach to dealing with issues in the online world to be critical given the globalised and decentralised nature of the internet.

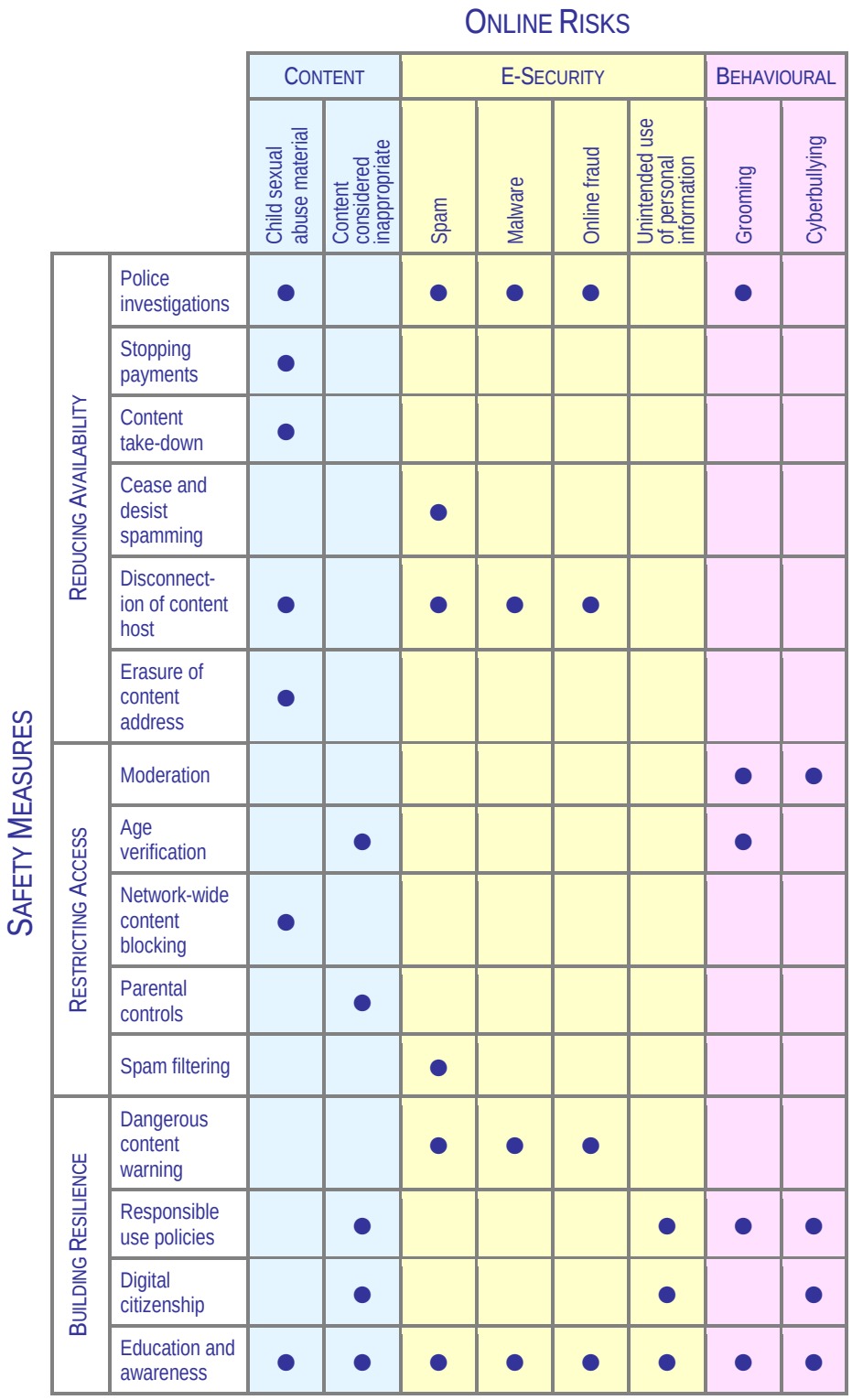
The Australian Government's response to the issue of online safety acknowledges the importance of education as a core component of an overall strategy. Our Cybersmart program aims to provide a comprehensive response to the cybersafety information needs of the Australian community, while the ACMA works with international and national stakeholders to ensure a co-ordinated approach (discussed further in response to TOR (iv) below).

The ACMA refers the Committee to the reports of its three-year program of research examining developments in cybersafety initiatives around the world aimed at protecting both young people and adults who access content on the internet. The three reports provide an in-depth analysis of the evolution of online risk in the emerging global digital economy. The reports explore a wide range of measures that can be deployed to mitigate online risk and promote online safety and capture the challenges in responding to online risk while user behaviour is constantly changing.

The 2007 report explored the development of the internet. It examined a range of measures used to minimise online risks. Notwithstanding the range of responses to online risks available the report noted that no single response will adequately mitigate all forms of online risk.

The 2008 report utilised a unified framework to examine safety measures that respond to online content, e-security and behavioural risks. The report uses the framework below to identify measures used to address risks. The report illustrates how the majority of measures that are used to mitigate online risk are relevant only for one or two types of risk category:

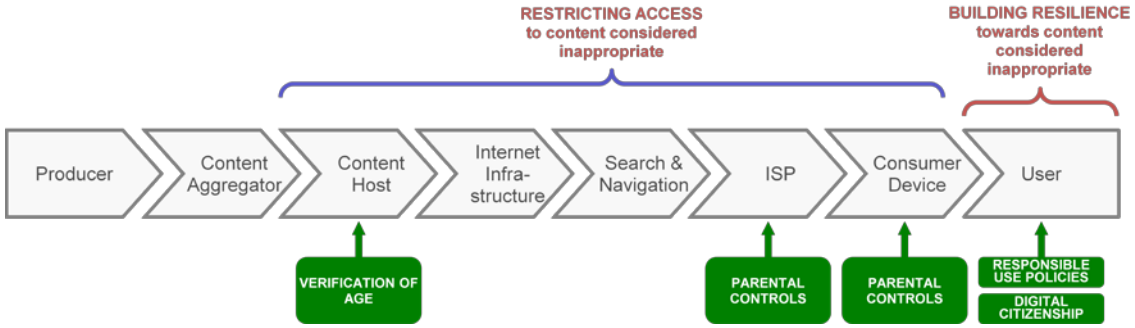
A framework for considering specific online risks and mitigation strategies



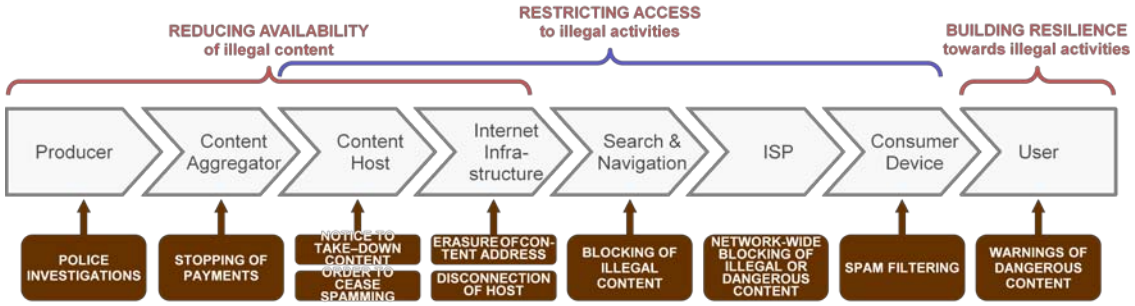
The 2008 report also noted the growing use of social media and associated risks of security of personal information, bullying and online fraud. It examines the criteria for evaluation of the effectiveness and influence of public awareness programs in bringing about behavioural change. It also examines the supply chain for internet content and services and identifies where in the supply chain safety measures can be delivered. It highlights how intervention at particular points in the supply chain can achieve the different objectives of:

- reducing the availability of illegal content; and
- restricting access or building resilience to illegal content and activity and content that may be considered inappropriate:

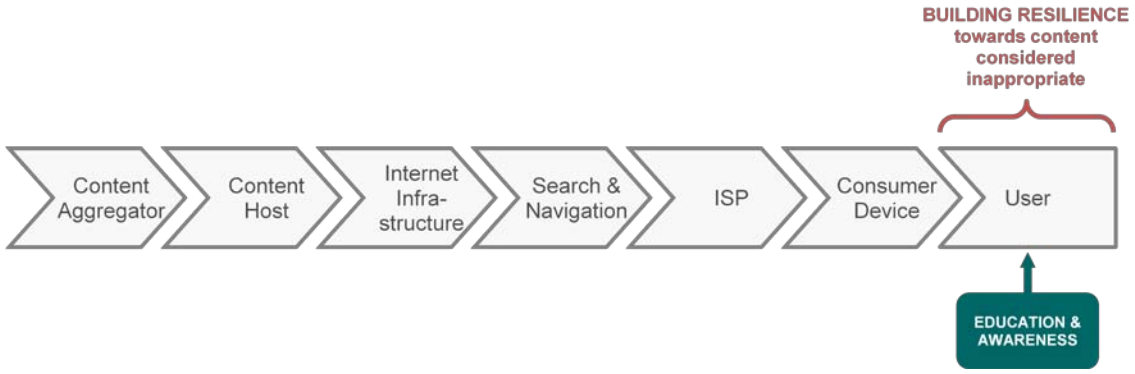
Points of intervention for measures to promote a safer online environment



Points of intervention for measures to reduce illegal activity



Points of intervention for measures to achieve public awareness



The 2009 report focussed on the way in which the use of ICT is embedded in the everyday life and behaviour of Australians, and noted that management of online risk has evolved in response to challenges posed by increased participation in the digital economy. The report highlighted the importance of building trust and confidence in the digital economy. It explored a response to online risk in Japan, dealing with the protection of 3G mobile users who are minors, and responses to concerns with Facebook's privacy practices, involving scrutiny by the Canadian privacy regulator and by Facebook's own user community. The report observed that separate but important contributions towards the effective management of online risk may be made by different players in the digital economy: governments and regulators; operators of online services; and users themselves.

The ACMA uses these reports, along with other research and data, to guide the development of a comprehensive range of high quality, evidence-based Cybersmart programs.

TOR(iv) Opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cyber-safety issues

The ACMA works closely with both international and Australian partners to ensure that its cybersafety programs are relevant, evidence based, and informed by best practice in cybersafety education. This "joined up" approach ensures that:

- messages and strategies are consistent across partners and delivery channels;
- resources are allocated according to areas of emerging needs; and
- gaps in the provision of cybersafety advice are identified and filled.

Under the *Broadcasting Services Act 1992* the ACMA has a formal responsibility to liaise with regulatory and other relevant bodies overseas to develop cooperative arrangements for the regulation of the internet industry. In the course of implementing Australia's co-regulatory scheme for internet content, the ACMA has participated in a range of international policy and regulatory forums.

The ACMA has had particular regard to the operation of the Safer Internet Action Plan (SIAP) of the European Union (EU), which has objectives and elements similar to the Australian co-regulatory scheme. The plan is comprised of strategies in the areas of hotlines, filtering, and education and awareness. International cooperation is encouraged as part of the program and the ACMA has well developed relationships with the two key arms of SIAP - INSAFE and International Association of Internet Hotlines (INHOPE):

- INSAFE is the international education and awareness network promoting safe, responsible use of the internet and mobile devices to young people. The ACMA is the Australian Safety Awareness Centre for this network.
- INHOPE provides a forum through which internet hotlines are able to exchange information and experience on matters such as complaint investigation processes, occupational health and safety for hotline staff, and standardised reporting of hotline statistics. INHOPE member hotlines deal with complaints regarding illegal internet content, particularly child sexual abuse material (sometimes referred to as child pornography), and the network is an effective mechanism for dealing with specific complaints and enhancing and complementing existing arrangements with law enforcement agencies. The ACMA has been an associate member since September 2002 and became a full member of INHOPE in May 2004.

Launched in September 2004, the Virtual Global Taskforce (VGT) is an international alliance of law enforcement agencies working together to make the internet safer for end users. ACMA is a partner to the VGT, which aims to deliver innovative crime prevention and crime reduction initiatives to prevent and deter individuals from committing on-line child abuse.

The ACMA has Memorandums of Understanding (MOUs) with key international partners, such as NetSafe in New Zealand and Childnet International in the UK. These are agencies that the ACMA has identified are producing best practice cybersafety resources. Through the MOUs, the ACMA has a platform for the exchange of information, research findings, and ideas, and collaboration around the production of cybersafety resources.

In the Australian context, the ACMA is a member of the Minister for Broadband, Communications and the Digital Economy's Consultative Working Group on Cybersafety (CWG), which provides advice to the Australian Government on cybersafety issues. The CWG brings together key stakeholders in the cybersafety arena and is valuable both in advising the government on future policy direction and ensuring existing programs are consistent and complementary. An example of CWG collaboration is the work undertaken annually around Safer Internet Day (discussed below). Another current

initiative is work being undertaken by the CWG on developing a common cybersafety help button, which will help ensure that Australians are able to readily access online help through a common interface.

Outside the CWG, the ACMA also works with key partners including education, industry, enforcement, and other organisations contributing to a safer online environment for young people. An example of this work is collaboration with the Alannah and Madeline Foundation on its Cybersafety and Well-being Initiative. This program aims to put in place a framework for the development of 'e-smart schools' which have the tools and knowledge to use technology safely. In providing schools with this tool kit of knowledge, the Alannah and Madeline Foundation links to the ACMA's resources and programs. This ensures that messages are consistent, and that programs complement and reinforce each other without unnecessary duplication.

The ACMA also regularly works with State Education Departments to raise awareness and promote common cybersafety messages. For example, the South Australian Department of Education and Children's Services recommends that school principals encourage their staff to attend the ACMA's PD for Educators program, inform parents and educators of the information provided by the ACMA and provide a direct link from the school's (or preschool's) website to the ACMA's website.

The West Australian Department of Education and Training is also working closely with the ACMA around the delivery of key cybersafety programs, including the Outreach program and Cybersmart Detectives. Such arrangements facilitate access by the education department to a comprehensive range of cybersafety resources, while providing the ACMA access to an extensive and effective delivery channel that is otherwise difficult to reach.

The ACMA is represented on a number of groups undertaking cybersafety-related research or programs, including the Technology and Well-Being Round Table and an initiative looking at the development of cybersafety resources for vulnerable youth.

While each group has a special area of expertise, in the ACMA's view it is important to ensure that the work of each builds on work already undertaken, as opposed to unnecessarily duplicating this work.

Hubs of activity

One area of focus for national and international networks has been the organisation of key events, or hubs of activity, that focus on online safety. Focused activities allow greater penetration of messages, which are able to be delivered through multiple platforms via various partner organisations. Examples of this approach are Safer Internet Day and National Cybersecurity Awareness Week:

Safer Internet Day	Organised by Insafe and originally a European based event, Safer Internet Day has expanded to involve over 50 countries worldwide, all promoting a common cybersafety message. With its international focus, Safer Internet Day is successful in building partnerships between participating countries and fostering an international perspective on safety issues. The ACMA is the Australian co-ordinator for Safer Internet Day events, and members of the Consultative Working Group (CWG) on Cybersafety have been active participants.
National Cybersecurity Awareness Week	National Cyber Security Awareness Week aims to help Australians understand cyber security risks and educate home and small business users on the simple steps they can take to protect personal and financial information. The ACMA hosted and participated in a number of events in the lead up to and during the week including launching a number of new programs and resources such as Cybersmart Hero, a new episode of Hector's World, the pre-service teacher training program and the new spam reporting tool 'Spam SMS'. The ACMA also participated in the Cyber-Security Roundtable for People with Disabilities, which was held at Parliament House.

The ACMA's access to world's best programs and resources

The ACMA's work with its international partners has given it access to world's best practice products and resources which it has adapted to suit an Australian audience. This ability to customise proven products for Australian audiences has been invaluable in assisting the ACMA in quickly delivering high quality programs in a cost effective manner.

ACMA programs are identified at Attachment A. Examples of where the ACMA has been able to adapt best practice international resources for Australian audiences include:

- Cybersmart Detectives (UK originated)
- Hector's World (New Zealand originated)
- Let's Fight it Together (UK originated)

"I thought the scenario was confronting (in a good way though) and really relevant particularly to this age group and considering how prevalent the new modes of communication are amongst kids and teens (chat rooms, email and mobile phones). Cybersmart Detective tied in really well with our previous work and really drove home the messages of protecting one's personal info, not trusting everything you're told/read on the Web and always checking with a responsible adult when they're unsure online" (Teacher, Victoria, May 2009)

...

"I learnt that giving out personal information can put you in a tricky situation and that people on the internet are not always who they say they are, playing the Cybersmart detectives games helps you learn" (student)

ACMA developed programs and resources

While the ACMA's relationships with various partners provides the opportunity to access the best cybersafety products and resources available and avoid a level of duplication which does not advantage Australian users, the ACMA also proactively identifies gaps and builds its own resources and programs from the ground up to suit the needs of Australians. Many of the resources and programs developed by the ACMA (and described further at Attachment A) are "world-firsts" including:

- PD for educators program;
- pre-service teacher training program;
- public libraries suite of resources[6]; and
- Cybersmart Hero – interactive anti-cyberbullying program

[6] Given the important role public libraries play in supporting local communities, the ACMA developed a suite of resources specifically for this sector. Resources include a printed Cybersafety guide for library staff, a printed Cybersafety guide for families, an A2 cyber rules poster and four on-line training videos for library staff addressing a range of technology related issues.

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

Access to, and use of, ICT is becoming essential for undertaking everyday economic and social transactions. The ACMA recognises the need to respond to the rapidly evolving opportunities presented by the new technologies in the digital economy to ensure consumers can be protected and the benefits of these technologies realised.

The ACMA's third report into online safety, *Online Risk and Safety in the Digital Economy* focussed on the use of ICT which is embedded in the everyday life and behaviour of Australians. It notes that management of online risk has evolved in response to challenges posed by increased participation in the digital economy. The report highlights the importance of building trust and confidence in the digital economy and discusses measures that have been developed to do so in relation to emerging mobile internet access platforms, the increased functionality of mobile phones and increased use of social media and online transactions across all ages.

The report illustrates this through a number of international initiatives, including:

- The Japan Safer Internet Program, where the government has set out a framework for the mobile internet of minimum standards for industry, and within which industry is encouraged to assist users to manage online risk through parental controls and adult media literacy programs.
- The Teachtoday portal, an industry-led response to concerns about cyberbullying of children and teachers.
- Social networking provider Facebook's response to its own stakeholder base—the users themselves—about protection of personal information, and Facebook's response to an investigation of its practice in protecting its user's personal information by the Canadian Office of the Privacy Commissioner.

Increasing community capacity and confidence in online engagement through risk mitigation and targeted awareness raising strategies is considered an important plank for increasing the productive use of ICT and level of Australians engagement in the digital economy.

The ACMA has developed competencies in the provision of targeted education and awareness programs through its cybersafety and cybersecurity activities. These activities are designed to allow Australians to take advantage of the economic and social opportunities provided by participation in digital communications. The ACMA is therefore well placed to build on these activities to ensure that the opportunities and economic benefits of use of new technologies by all Australians are maximised.

TOR (vi) Ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying including by:

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

The ACMA's Cybersmart programs assist schools to identify and manage cybersafety risks by empowering teachers, students and parents with the knowledge, skills and strategies to effectively address cyberbullying issues.

The ACMA's programs assist schools in developing consistent whole-school approaches to cybersafety by working with the entire school community, including parents, to adopt protective and preventative strategies. The ACMA has also recently conducted a study examining the cybersafety information needs of parents. This study is being used as the foundation to develop a new set of resources for parents on the Cybersmart site. The PD for Educators, pre-service teacher training program and Internet Safety Awareness Presentations for students, parents and teachers all include content specifically directed at reducing the incidence and harmful effects of cyberbullying, including the development of policies and procedures to better address this risk.

Feedback and informal evaluation of programs to date demonstrates that the ACMA's programs are assisting schools, parents and students in responding to cyberbullying and other online risks:

> ***"Just to let you know the two presentations were brilliant. The staff and students alike were very impressed - and concerned. I wish I had a dollar for every student who came up to me and said she was going home to change her Myspace/Face book etc page - just what I wanted!!!" (High school teacher, Sydney, 2009)***
>
> ...
>
> ***"The impact you had in our school is still ongoing. The students and staff were talking about your presentations in a very positive manner. What is surprising is the longer term impact it has had on kids. Most of our Year 12 students have now selected cyberbullying as their research topic for ethics in English. (Principal, Tasmania, 2008.)***

The full range of ACMA Cybersmart programs are described at Attachment A. Those most relevant to this term of reference are:

- Professional Development for Educators;
- Internet Safety Awareness Presentations for students, parents and teachers;
- Cybersmart Online Helpline
- Cybersmart Hero;
- Hector's World;
- Wise up to IT; and
- Let's Fight it Together.

TOR (vii) Analysing information on achieving and continuing world's best practice safeguards

A significant body of work, including research and external evaluation, is undertaken by the ACMA to ensure the continued relevance, development and enhancement of its cybersafety education resources and programs.

For example, the *Click and Connect* research was undertaken by the ACMA to further explore trends identified in its earlier reports of the children's use of online technologies, and to inform the development and enhancement of ACMA's cybersafety program. When released *Click and Connect* was the most comprehensive quantitative research in Australia of parents and children in the 8-17 age group. It helped shape relevant, current safety messages for young people, teachers and parents by providing information on the issues currently facing young people online, including their understanding and experience of risks, and the ways in which they manage these risks.

The findings continue to directly influence the development and enhancement of program material. Looking to the future, for example, the ACMA will draw on the *Click and Connect* research to develop safety initiatives for the more vulnerable subgroups of young people, particularly those aged 14-17, who are aware of the risks of certain online behaviours, but engage in risky behaviour regardless.

The ACMA has recently commissioned formal and independent evaluations of a number of its programs to measure their effectiveness and ascertain how they can be further enhanced. Programs being evaluated include Cybersafety Outreach and Cybersmart Detectives.

In doing so the ACMA is aware that the development of frameworks for rigorous assessment of programs has been an underdeveloped area. The ACMA observed in its 2008 report into developments in online safety initiatives around the world, that there was little empirical data currently available to benchmark the effect of cybersafety education and awareness programs, in terms of:

- the impact of the messages being delivered
- the utility of various delivery mechanisms, and
- the degree to which the programs contribute to achieving the desired short and long term behavioural outcomes.

That report explored characteristics that might constitute an 'effective' cybersafety program—that is, what key features should be present within a product or program in order for it to be more likely to be effective or influential. These are informed by the broader principles of educational or behavioural theory, rather than being specific to the online environment.

The report refers to the work of Luna and Finkelhor, (University of New Hampshire in the US) around their evaluation of school-based child victimisation prevention programs[7] as well as the report produced for the former Commonwealth Department of Education, Training and Youth Affairs' review of effective national and international intervention strategies to assist at-risk students and reduce early school leaving.[8]

[7] *School Based Prevention Programs: Lessons for Child Victimisation Prevention*, Luna, R and Finkelhor, D, Durham, NH: Crimes Against Children Research Center, (1998) (http://www.unh.edu/ccrc/pdf/CV30.pdf) (accessed 15/9/2008)

[8] *Innovation and Best Practice in Schools: Review of Literature and Practice*, Strategic Partners in association with the Centre for Youth Affairs., prepared for the Commonwealth Department of Education, Training and Youth Affairs, February 2001

A synthesis of these reports reveals a number of key relevant features stand out, forming a framework for evaluation. These indicate that an effective awareness program should:

- deal with issues identified through robust, current research;
- be based on sound developmental and behavioural foundations;
- adopt an approach which increases knowledge and skills;
- comprise multiple components, allowing for a variety of approaches to consolidate the messages being imparted and to reinforce the desired behavioural traits;
- be empowering, not relying solely on fear tactics; and
- be developed in collaboration with partners.

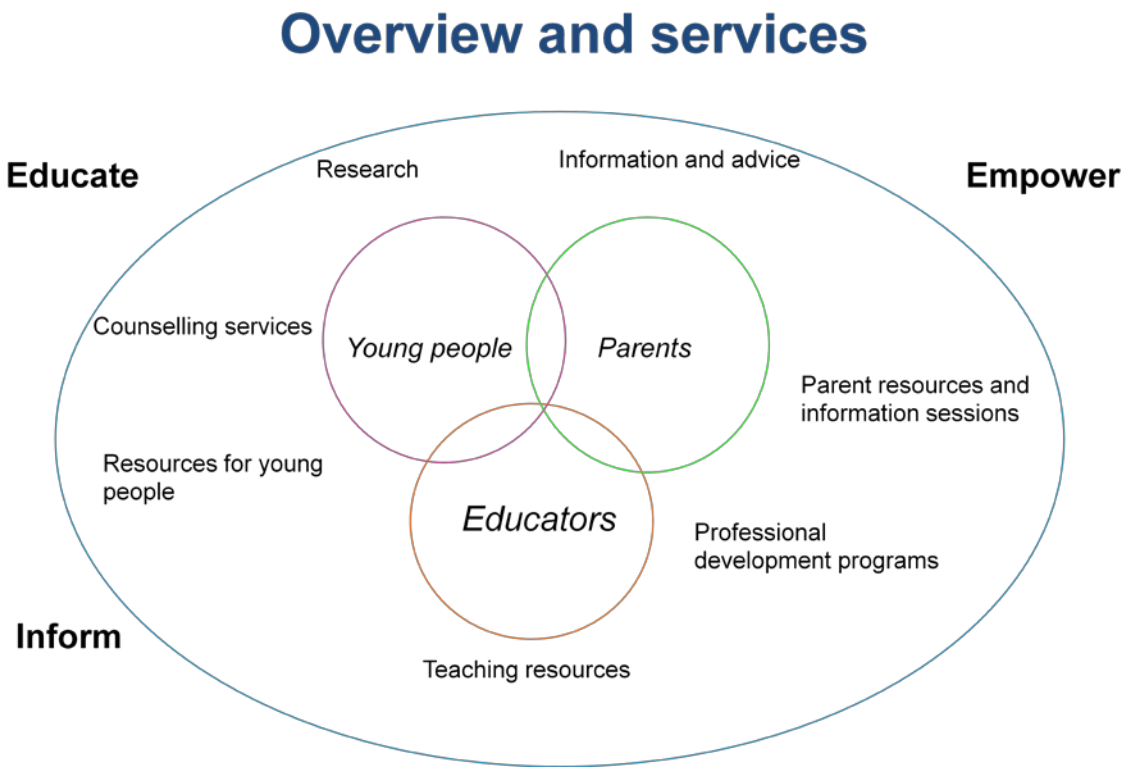
http://www.dest.gov.au/sectors/school_education/publications_resources/profiles/innovation_and_best_practice_in_schools.htm#versionAvailable (accessed 16/9/2008)

ACMA Cybersafety Programs

Under the brand name Cybersmart, the ACMA provides a diverse suite of cybersafety programs for young people and for key stakeholders who are able to influence young people's online engagement - parents, teachers, trainee teachers and librarians. The ACMA's Cybersmart programs are built on a firm evidentiary base and adhere to strong education and learning principles.

In developing its Cybersmart programs, the ACMA has aimed to construct a broad based program, with multiple elements targeting the needs of particular audiences (see Diagram 1 below).

Diagram 1: ACMA's Cybersmart programs: Framework



As Diagram 1 indicates, the ACMA's Cybersmart programs aim to *inform, educate and empower* young people, to enable them to safely navigate the online world and be active, effective digital citizens. The ACMA's approach is to ensure its programs are based on research into young people's online behaviour, the risks they face, and to provide viable strategies for managing risk. In turn, the ACMA is able to access valuable front-line intelligence from its Cybersafety Trainers in the field to be alerted to emerging issues and trends and to further enhance the Cybersmart programs and resources.

The ACMA's Cybersmart Website

The Cybersmart Website (www.cybersmart.gov.au) is the cornerstone of the ACMA's Cybersmart program. A screen shot of the homepage has been provided as Diagram 2.

Diagram 2: The ACMA's Cybersmart website homepage

The website acts as a one-stop shop for general cybersafety information, with information targeted to six specific audiences - young kids, kids, teens, parents, teachers and librarians:

For Young people Tips and advice on online behaviour, fun activities such as quizzes and animations, and high quality, interactive education resources for use in the classroom. The website also hosts a series of cybersafety videos made by young people for young people, as part of the ACMA sponsored *Screen It* film competition held in 2009.

For Parents The website offers a practical guide to their child's online use, which aims to demystify the online world and encourage parents to actively engage in this world along with their children. Information and advice is accompanied by videos in which parents talk about their online experiences and provide practical pointers for other parents. Following research into parents' cybersafety information needs undertaken in December 2009, the ACMA is now building on its set of parent materials to ensure that parents can easily access relevant information based on the age of their child.

For Teachers

The website contains the Schools Gateway – a comprehensive, age based education resource for teachers, including interactive education resources, lesson plans, a guide to students' use of technology, and links to cybersafety policies and procedures from education jurisdictions throughout Australia.

Key education resources available from the Schools Gateway include:

- Hector's World: for younger primary school
- Cyberquoll: for upper primary school
- Cybersmart Detectives and Cybersmart Hero: for upper primary school.
- Cybernetrix: for lower secondary school
- Let's Fight it Together: for lower secondary school
- Wise Up to IT: for mid to late secondary school students

All resources feature age appropriate safety advice and comprehensive, ready-to-go lesson plans.

For Librarians

The ACMA has developed a range of resources about how to manage risks so that library users have safe and positive experiences online. Developed in conjunction with the Australian Library and Information Association and Australian Public Libraries these resources aim to complement existing policies in libraries and provide additional resources and support to library staff.

Hard copy cybersafety resources

Education resources and general safety advisory material is available in hard copy as well as online. In 2009-10, the ACMA distributed over a million hard copies of its education resources and advisory brochures to schools, parents and community groups throughout Australia (hard copies of the ACMA's resources can be ordered free of charge through the website or by calling the ACMA's Cybersafety Contact Centre on 1800 880 176).

The Cybersafety Outreach Program

Complementing and building on the website information, the Cybersafety Outreach program delivers face-to-face presentations to audiences of students, parents and teachers. Delivered without charge and Australia wide, the three programs are currently available:

- Professional Development (PD) for Educators program
- Internet Safety Awareness Presentations for teachers, students and parents; and
- Pre-service teacher training program (launched in June this year).

There is a high level of demand for Cybersafety Outreach events with presentations and workshops booked six months in advance. Further, demand for the program continues to grow with 20,000 students, parents and teachers participating in an Outreach event in May 2010 compared to 5,000 in May the previous year.

Since January 2009 over 5,100 teachers have participated in the full day PD workshops and 131,902 teachers, students and parents have attended the one hour presentations. During this time 2,366 schools have participated in Cybersafety Outreach events across Australia.

Professional Development (PD) for Educators program

The PD for Educators program was carefully developed in consultation with key stakeholders and education bodies and launched by the ACMA in January 2009. This full-day workshop provides teachers with a comprehensive understanding of a modern student's technology profile, digital literacy, positive online behaviour, personal and peer safety and the legal obligations of schools and teachers to minimise and address risks.

Teachers who attend the PD advise the ACMA that as a result they are:

- better equipped with the tools and confidence to engage students on cybersafety issues
- able to incorporate strategies into the curriculum to keep students safe at all year levels
- aware of the capabilities required to develop good digital citizens
- better able to identify and prevent cyberbullying
- better able to use ACMA teaching resources—including the example school policies, case studies, lesson plans, video resources and more.

The PD program is accredited or endorsed in all states and territories and is available in all regional and metropolitan areas across Australia. Delivered by an experienced cybersafety trainer with an education background, the PD program is offered as either a workshop held at a particular school, or an off-site workshop held at a local venue.

Feedback from PD participants continues to be very positive with 99% of participants rating the program as either "excellent" of "very good". The PD program is an area where Australia led the world in the provision of comprehensive cybersafety education, and the ACMA's program has attracted considerable international attention.

An interactive e-learning platform building on the PD program is to be offered later in 2010. It will give teachers and schools increased flexibility in accessing critical cybersafety information. This will enable greater access to the program for all teachers including those who are unable to attend face-to-face sessions because of their geographical isolation or for other reasons. The ACMA expects casual relief teaching staff will also benefit from the e-learning program.

> ***"An informative and helpful workshop. The activities were practical and helpful for clarifying different areas that need attention. As my focus is on education and a preventative slant I really appreciate the information. It will assist me to see areas that we can improve on in educating our kids and understanding the pressures our kids are under" (Teacher, Qld, 2010)***
>
> ***…***
>
> ***"I found the content of this PD very relevant to me as both a parent and teacher. It has given me some good ideas with my classes and also with parents when we introduce out virtual classroom to them" (Teacher, Qld, 2010)***
>
> ***…***

"I like the idea of running forums to educate parents, teachers. IT managers speaking to year groups sounds great. The overall day was really useful and informative and gave a clear overall picture of many of the issues facing children teachers and parents. All the lecturer's examples were very interesting. There is a lot to think about and act on and all the handouts, resources etc will be very useful." (Teacher, WA, 2010)

Pre-service teacher training program

An extension of the highly successful PD program, the ACMA recently launched its pre-service teacher training program. This is a national program designed for education students in their final year at university. The 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, identity protection and responsible digital citizenship.

Consisting of a 50 minute resource lecture and a 90 minute tutorial, the pre-service teacher program is the result of extensive consultation with key stakeholders and the university sector. The program's effectiveness was thoroughly tested during a pilot program attended by more than 550 pre-service teachers in October 2009.

"I found the lecture fantastic and really caused me to think about and relate to the content discussed. A great resource for new teachers and students" (Australian Catholic University student, 2009)

...

"A fantastic presentation – very well created and presented and highly relevant. Resources are great and easily accessible" (Deakin University student, 2010)

Internet Safety Awareness Presentations

The ACMA also provides Internet Safety Awareness Presentations (ISAPs) in support of a whole-school approach to cybersafety education. An ACMA Cybersafety Trainer provides 45–90 minute presentations on cybersafety issues for students, parents and teachers. These presentations are adapted to suit the different audiences (and ages of the student groups). The presentations are easy to understand, non-alarmist, thorough and informative. They cover a range of issues including:

- the ways children use the internet and emerging technologies;
- potential risks faced by children when online such as cyberbullying, identity theft, inappropriate contact and exposure to inappropriate content; and
- tips and strategies to help children stay safe online.

"After the presentation to students yesterday, we were all talking about the risks. My friends and I decided we would all put in place the safety measures you mentioned. We organised to meet on line in Bebo at 8:00 pm and make our sites private at the same time. We used the chat features of Bebo and texting on our phones to check we still had access to each other's sites. There was about 90 of us who all met at the same time and made the changes" (Year 8 student, Qld, 2008.)

...

"My daughter (year 11) changed her Facebook page following this presentation. It made her aware of the pictures and information she was putting on her Facebook page. Many of her friends changed their pages too. She is now happy for me to be one of her 'friends' and view her site whenever I wish to. I continue to remind her of the 'talk' and it is still clearly in her mind. Thank you" (Parent, March, 2010)

...

"I am sure you hear this all the time but your presentation was amazing. Any of us who are involved in the education of children hope that we make a difference. Not all of us are as assured of achieving it as you. I cannot describe to you the vibe in the School after you left. A number of very long serving staff (me being one of them) could not remember any event that resonated throughout the School in the way you did. Thank you so much for all that you have done for our girls in the pursuit of keeping our young people safe". (Teacher, Victoria, 2008.)

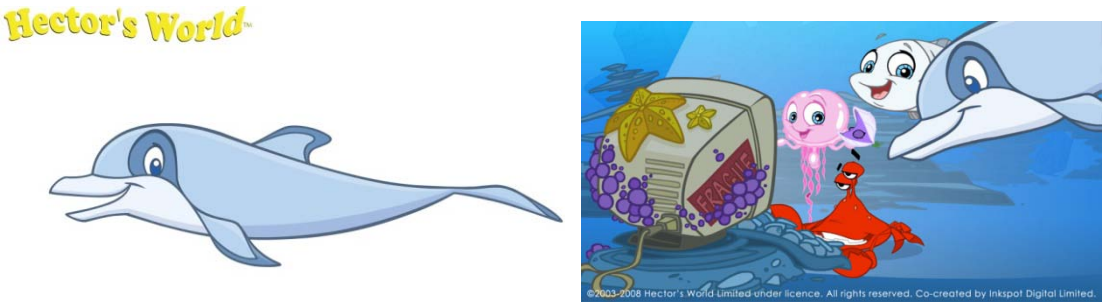
Cybersmart Online Helpline

For young people who need in-depth assistance following a negative online experience, the ACMA operates the Cybersmart Online Helpline. Young people experiencing issues such as cyberbullying, the misuse of personal information online, or exposure to offensive content or unwanted contact, are able to access free, confidential online counselling. This service is provided in conjunction with the Kids Helpline, specialist providers of counselling services for children and young people.

Cybersafety Contact Centre - 1800 880 176

For parents, teachers or others with general enquiries about cybersafety issues, the ACMA also operates the Cybersafety Contact Centre, a nationwide 1800 number advisory service (1800 880 176). In addition to assisting callers with general cybersafety enquiries, this service enables callers to book Outreach presentations or order cybersafety resources for use in their school or community group.

Hector's World



Pitched at younger children aged 2 to 10 years, the interactive episode explores the impact that cyberbullying can have on someone and encourages targets of cyberbullying to contact a trusted adult for help. The story encourages bystanders to see cyberbullying as unacceptable behaviour and to refrain from becoming involved in bullying.

> *"A very engaging and appealing (fun) way of getting a very serious message across. The students love it and are learning so much!" (Teacher, Northern Territory)*
>
> *...*
>
> *"Up till now this is the best thing in my world. I learned that you should always use the internet with a grown up" (student, Year 1, NSW school)*
>
> *...*
>
> *"I like Hector's World because it's funny! I learned that you should ask a grown up if you want to go on the internet and to delete bullying (messages)" (student, Year 1, NSW school)*

CyberQuoll

The internet-related antics of the Quoll cousins are the focus of this internet safety resource for upper primary school students. CyberQuoll provides users with a fun, cartoon-style multimedia experience with episodes covering the basics of internet use and how to keep safe online. CyberQuoll includes a range of teacher materials such as a Teacher Guide, student worksheets, certificates and contracts. CyberQuoll also includes materials that parents can use with their children at home.

Cybersmart Detectives

Cybersmart Detectives is an innovative online activity that teaches children key internet safety messages in a protected environment. Students work online and in real time, liaising with community professionals to solve an internet-themed problem. The aim of

the program is to educate and empower students to make more informed decisions in real life situations.

In the activity, students assume the role of an onlooker in their current year at a fictional local secondary school. They are concerned about the welfare of a student at the school, particularly with that student's online activities. Guided by a series of clues, students work collaboratively in teams to solve a mystery. Cybersmart Guides respond to the questions and theories posed by the students and guide the teams through each of the 'clues'.

As the scenario unfolds, the students discuss the risks of certain online and offline behaviours, and ways of managing those risks. Although the scenario presented in the activity is simulated, the sense of urgency that excites students taking part is very real.

By the end of the activity students will have learned:

- valuable lessons about some of the risks associated with internet use
- useful tips for chatting safely online

Cybersmart Hero

A sister program to Cybersmart Detectives, Cybersmart Hero is an interactive online activity that teaches children about cyberbullying in a protected environment.

Students work online, and in real time, liaising with community professionals to respond to a cyberbullying issue. The aim of the program is to educate and empower students to make informed decisions in real life situations.

In the activity, students play the role of a bystander who becomes aware of a cyberbullying problem at school. Students ultimately become concerned about the welfare of a fellow student, who is the subject of some targeted bullying through electronic media such as texts, emails, chat rooms and social networking.

As the scenario unfolds, the students are required to discuss the issues and make decisions about the responsible course of action. By the end of the activity students will be familiar with the issues around cyberbullying and how to respond to those issues if they are ever faced with similar situations.

CyberNetrix

Designed for early teens, CyberNetrix is an engaging multimedia resource which includes interactive activities designed to simulate popular online activities such as instant messaging. CyberNetrix aims to highlight age-specific risks online and offer advice on how to avoid them. This resource includes a Teacher Guide with activity guidelines and student handouts.

Wise up to IT

Wise up to IT is a video-based program aimed at secondary school students. The program covers cyberbullying, online stalking, internet security and grooming in four videos which depict young people's experiences online. The videos encourage students to think about who they are really chatting to online, what personal information they are posting and whether or not their computer is protected from scams and spyware. Wise up to IT is supported by teacher and student resources and is available both as a DVD and online.

"Some students wanted to watch and discuss it several times" (Teacher, SA)

...

"Very confronting and made children think deeply about what they do on the internet" (Teacher, SA)

Let's Fight it Together

A comprehensive teaching resource including a seven minute film and a user guide with lesson plans for teachers, and tips for parents and carers. The film depicts the story of a teenager who becomes the target of bullying via the internet and his mobile phone. The film shows how cyberbullying might occur, who it involves, the impact it can have, and how it might be resolved. Let's Fight It Together can help young people, their parents or carers and teachers better understand the issues surrounding cyberbullying.

"Brilliant, very responsive from students, real –life (great clip). Excellent and well supported lesson plans" (Teacher, NSW)

...

"The lesson plans / support material for this resource was very detailed. It allows staff members to feel confident in implementing it. Schools are such busy places it was great to grab this resource and get into it" (Teacher, NSW)

...

"Showed the film [Let's Fight it Together] to the whole school. Students were enthralled and followed intensely. In fact they described it as "awesome"." (Teacher, Northern Territory, 2009)

...

"Students responded very well [to Let's Fight it Together], showing great empathy across the year groups. Not a sound was heard from the students whilst they viewed it. The case studies were also brilliant" (teacher, NSW, 2009)