DIRECTOR GENERAL SUBMISSION REGARDING THE JOINT SELECT COMMITTEE ON CYBER SAFETY INQUIRY INTO CYBER SAFETY

The Department of Education, Western Australia takes all forms of bullying seriously. Along with establishing partnerships with key stakeholders to address the problems of bullying, school communities are supported with policies to assist with incidents of bullying, and with preventative strategies and programs.

The Department of Education uses the following definition of cyber bullying.

Definition: Cyber bullying is when an individual or group misuses information and communication technologies such as email, text messages, instant messaging and websites to engage in the bullying of other individuals or groups.

Bullying takes many forms and can include:

- Verbal Bullying: the repeated use of words to hurt or humiliate another individual or group. Verbal bullying includes using put-downs, insulting language name-calling swearing, nasty notes and homophobic, racist or sexist comments.
- Psychological Bullying: includes repeated stalking, threats or implied threats, unwanted email or text messaging, abusive websites, threatening gestures, manipulation, emotional blackmail, and threats to an individual's reputation and sense of safety.
- Relational Bullying: usually involves repeatedly ostracising others by leaving them out or convincing others to exclude or reject another individual or group from their social connections, making up or spreading rumours and sharing or threatening to share another's personal information.

The use of technology provides an alternative means for verbal, relational and psychological bullying to occur, facilitating the covert nature of cyber bullying. Cyber bullying is cruel and insidious in nature, and is difficult for students, parents or schools to manage in isolation. It requires a response that addresses the social dynamics which underpin this behaviour.

The Australian Covert Bullying Prevalence Study conducted by the Child Health Promotion Research Centre (CHPRC) at Edith Cowan University indicated that the level of cyber bullying is related to age in relation to access to technology – the older children become, the greater access they have to technology. A number of further studies exploring the issue of bullying conducted by the CHPRC indicated that one in four Australian children reported being bullied at least every few weeks if not more often. In relation to cyber bullying, rates could be as high as one in every three Australian children, influenced by age and access to technology, with older students more likely to engage in cyber bullying than younger students. The occurrence of cyber bullying in the home is more significant the older the student especially if parents don't have the knowledge and skills to assist and support their child.

Data that was collected by the CHPRC during Terms 2 and 3 of 2008 from 2 400 students from 40 Western Australian schools across the state and sectors showed the following:

- Students who are cyber bullied are:
  - 13 times more likely to be bullied face-to-face;
  - four times more likely to cyber bully others and twice as likely to bully others face-to-face;
  - twice as likely to have their own mobile phone and nearly twice as likely to have wireless internet at home; and
  - nearly twice as likely to report poor school grades.

- Students who cyber bully others are:
  o 18 times more likely to bully others face-to-face;
  o four times more likely to be cyber bullied;
  o nearly three times more likely to have their own mobile phone; and
  o more likely to think cyber bullying is okay.
- Mobile phones are most commonly used for cyber bullying among adolescents in Australia.
- According to the research findings cyber bullying has a greater impact on those being bullied than traditional face-to-face bullying.

The nature of cyber bullying means that the amount of time students can be exposed to bullying behaviours has increased. Whereas previously students who were bullied at school could feel safe at home, the advent of cyber bullying means this is no longer the case. It has also made it possible for students to be anonymous in their bullying. This can make it very difficult to address. Evidence is indicating that some students who would not engage in bullying behaviour face-to-face will participate in cyber bullying because of the anonymity.

The role of the school in relation to cyber bullying that is occurring outside of school hours and subsequently impacting on the school day can blur the lines of responsibility. Increasingly the demand is on schools to deal with issues that occur outside of school hours irrespective of whether it has a direct impact on the well being of the school population or not. The Department would endorse the development of clear advice regarding this issue.

The Department of Education has implemented a tiered approach to filtering Internet access in order to minimise the risk of student and staff exposure to inappropriate Internet content.

At a system level, the Department has implemented a central filtering service based on blocking access to approximately 750 000 sites that have been identified as containing content that is unsuitable for the education market. This centrally managed blacklist service is linked to other similar services around the globe and is updated daily to reflect changes occurring on the Internet.

At a local network level, each school has an Internet filtering device which enables a further level of Internet access filtering to be put in place. Schools manage this level of filtering locally in order to best meet their school needs.

Computers used on school networks are supplied with Internet browser software default settings that are pre-configured to block certain actions that may inadvertently lead to displaying materials containing sexual content. Similarly, most online search engine services, such as Google, Yahoo and Bing have a default 'safe search' setting which can filter out most adult materials including video and image search results. In most cases, local browser and search engine preferences can be modified locally to apply varying degrees of protection from adult content. Google has a number of articles relating to Google's own SafeSearch filtering choices which can be made within the Google browser settings area on any workstation.

The Department of Education has developed a *Students Online* policy to assist teachers to put in place school-based processes and procedures that both protect and inform students and inform students and parents in their use of Departmental online services. The Department continues to work with The Australian Communications and Media Authority's (ACMA) Cybersmart initiative – a Federal Government supported Internet safety advisory body established to provide independent advice and education on managing access to online content.

Unfortunately, the scale and inherent nature of the Internet is such that no filtering mechanism can offer guaranteed protection from all content that may be considered inappropriate in a school setting. However, when used in conjunction with user awareness, agreed operating procedures and adequate supervisory techniques in the classroom, the combination of these technologies and practices provide a high level of protection and an understanding of how to use the Internet appropriately and safely.

The Department of Education has been active in pursuing opportunities for cooperation across Australian stakeholders in dealing with cyber safety issues. Firm links have been established with ACMA and the Australian Federal Police who provide schools the opportunity of accessing *Cyber Safety Outreach* programs. The Department has a key role in the coordination of the Cybersmart Detectives online activity developed and presented by ACMA. The Department liaises between ACMA, Catholic Education Office WA and Australian Independent Schools Western Australia to ensure all primary schools, public and private, are able to access the activity. The *Cyber Safety Outreach* program has demonstrated very effective outcomes and as such is in constant demand by schools. However, the current configuration of one presenter to support South Australia and Western Australia is impractical when considering the geography of Western Australia.

The Department welcomes ACMA's planned on-line training for teachers and the opportunity to be involved.

The Department has worked with the Alannah and Madeline Foundation to support the *Cyber Safety and Wellbeing Initiative*, funded by the Federal Department of Education, Employment and Workplace Relations. The initiative aims to help schools to create a cultural norm of smart, safe and responsible use of communications technologies. Along with guidance for schools regarding appropriate teaching resources on cyber safety, the initiative will support schools to make the links between technology and wellbeing issues. Several Western Australian public, independent and Catholic schools have been supported in their application for available grants.

To celebrate *Safer Internet Day*, a worldwide activity, the Department in conjunction with the ACMA invited public schools in Western Australia to participate in a variety of activities including a national Cybersmart Detectives activity. Schools were able access a range of activities and resources for students of all ages including interactive educational programs with teacher and student resources such as teacher guides, lesson plans and activities. Although a beneficial event, *Safer Internet Day* is organised to suit the school calendar for the northern hemisphere. In Australia it falls at the beginning of the school year with many schools opting not to participate due to already busy schedules.

The Department has been active in supporting the *Bullying No Way* website both with funding and input into the development of online curriculum materials.

The Department of Education works closely with the CHPRC in research projects looking at the nature, effect and prevention of bullying including cyber bullying. Some of this research culminated in the development of the *Friendly Schools and Families* materials. A large number of public primary schools in Western Australia are now implementing this approach successfully to reduce and prevent bullying.

As the culmination of the cyber bullying research conducted by the CHPRC, 200 Year 10 students were involved in a cyber summit. One of the main aims of the summit was to engage students in problem solving around the issue of cyber bullying. The results of the summit were presented to the Minister for Education in the form of a Declaration. The ideas outlined in this document demonstrate the willingness of young people to own the problem and to develop their own solutions. Having students generate solutions is the most powerful strategy to combat cyber bullying. It is only by working with our young people that we will find the solutions that can make a difference. The Victorian Department of Education has conducted a summit based on this model.

The Department has aligned its policy and practice about using or banning social networking sites with the advice of experts in cyber safety such as Professor Donna Cross. The position is one of supporting teachers to be well informed and understand how the sites work before using them with students. Protective behaviour curriculum needs to include the teaching of skills to increase privacy settings on these sites, to know how to report inappropriate postings and to reduce any risk of harm. Through a partnership with Online Curriculum Services and branches of Student Services, the Department has developed a series of Protective Behaviours resources for teachers and an online professional learning is being produced that will address some of these issues. Work is underway in the Online Curriculum Services Branch to produce collaboration and social networking services that are contained and managed within the Department's network.

The Online Curriculum Services Team is preparing a series of advice papers that bring together information about policy interpretation, details about the social networking application and curriculum advice on how to use the application for engaging student learning. These resources will be delivered as training modules and then also made available as online resources.

Teachers enrolled in the Department of Education's *Teachers have Class* program can access a self paced online course about the use of wikis, blogs and other social networking sites. There are 2 500 public teachers enrolled in this program. Teachers have stated they need this level of practical support to understand the risks they undertake when using public sites in the classroom.

The Department of Education convened the Cyber Safety for Children Working Party in 2008. The first of its type nationally, this cross sectoral and inter-agency group draws together key stakeholders whose purpose is to:

- support activities for promoting student Internet safety in school communities;
- provide advice about and support for strategic initiatives for promoting children's and young people's Internet safety in the wider community;
- share information across systems and sectors about policies and initiatives that impact on Internet safety; and,
- provide a forum for discussion and application of research relating to best practice in cyber safety.

The Cyber Safety for Children Working Party would prove ideal as a forum for the discussion and application of the findings of the inquiry.

Relationships have been established with the Office of Crime Prevention and WA Police to specifically address 'Sexting.' The working party was formed in response to incidence of sexting that have occurred in schools where it was evident that measures to maintain the well being of the students and the integrity of the schools involved were required.

In collaboration with WA Police a Police Schools Safety Liaison Officer was appointed to the Department of Education to support schools in keeping their communities safe. The Police Schools Safety Liaison Officer is available to assist schools in managing cyber issues including sexting and extreme cases of bullying and intimidation.

Clear instructions have been issued to public schools about the use of mobile phones and the internet. As a minimum mobile phones must be switched off in classrooms. Additionally it is expected that school principals will suspend any students found to be involved in recording, distributing or uploading inappropriate images. With community consultation public schools are also able to ban mobile phone use anywhere on the school site, if that is considered necessary.

The Department of is committed to the care, safety and protection of all children attending public schools. The Department's *Child Protection* policy explains the actions to be taken by staff to protect children in circumstances where abuse is suspected. All staff have an important role in the identification and reporting of child abuse and the provision of support and assistance to children who have been abused.

Child protection and the prevention of child abuse is an across government initiative and a shared community responsibility. The *Child Protection* policy recognises that the best interests of children will be met by collaborating with or engaging the expertise of other government agencies or non government departments in accordance with existing protocols.

Under the *Child Protection* policy, the use of electronic devices for the purposes of the distribution of sexually explicit material, solicitation and harassment constitutes child abuse and/or criminal behaviour that must be reported to the principal. The protection of children from sexual and emotional abuse perpetrated through the use of electronic means is managed through security software, computer access and mobile phone policies, school education programs and by reporting incidents.

The Department has developed an online child protection professional learning program for all department staff on child protection and mandatory reporting legislation. The online learning program is designed to help protect the safety and wellbeing of students by ensuring school staff:

- have the appropriate professional knowledge and understanding of child protection;
- understand their responsibilities under the mandatory reporting legislation; and
- understand their responsibilities under the Department's *Child Protection* policy and procedures.

The Department acknowledges that students are potentially exposed to a wide range of situations that put them at risk and cause them short and long term physical and emotional harm. Teaching preventative strategies is a proactive way to strengthen students' ability to keep safe and minimise risk.

The *Protective Behaviours in Schools Project* is a joint initiative of Protective Behaviours WA Incorporated and the Department of Education. The *Protective Behaviours in Schools Project* is a life skills and personal safety program which aims to strengthen the resilience of students. Protective Behaviours focuses on giving students skills and strategies to protect them from abusive and potentially unsafe situations.

The Department is developing a Protective Behaviours curriculum package that is embedded in the Health and Physical Education curriculum. An online professional learning program in Protective Behaviours is being developed for teachers and is scheduled for release in 2011.

The Department of Education, Western Australia recommends that:

- any recommended actions be based on research and evidence;
- a coordinated and collective effort between the community and the government be endorsed by the Joint Select Committee;
- the Joint Select Committee supports an increase in funding to continue research and to provide additional funding to support the extension of such programs as the Cybersmart Detectives Outreach and the Bullying No Way website; and
- The Joint Select Committee considers the mandating of Cyber safety training for all educators including pre-service teachers.