

Joint Select Committee on Cyber-Safety

New South Wales Secondary Principals' Council response to the Areas of Interest identified by the Joint Select Committee on Cyber-Safety.

a)

- (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)

Government has a key role in legislating to ensure providers are legally responsible for acting on requests to remove material from their sites – whether they are in Australia or elsewhere. Internet service providers and content service providers have a commercial opportunity to provide a range of products with a variety of different filters and controls to enable parents to manage the home environment.

Government has a role in providing information to parents to enable them to make safe choices for their children in the home environment. Parents need to be given the tools to manage the online environment in the home environment where less rigid filters and controls are often in place. www.cybersmart.gov.au is a good start but needs wider advertising to parents and further development and expansion

Local government has a role in providing appropriately filtered access through public libraries and other public facilities.

The NSW SPC:-

- recognises that the environment of public schools in NSW is managed with filters that control the access to the online environment. The control of those filters is continuously monitored and evaluated in public schools and needs to be managed similarly in the private school environment. Consideration does need to be given to differentiating the filters between staff and students. It is very difficult for school personnel to follow-up an issue when the site where the issue is identified is blocked to staff.
- agrees that teachers are in a unique position to influence the engagement of students in the online environment. The relevance and timing of this instruction needs to be carefully considered. Schools already take advantage of opportunities to provide information to students and families and do not need this to be legislated.

- (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 (eg technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking)
- Identity theft

- Breaches of privacy

The places where those controls are at greatest risk are the home and mobile environments. Children and young people are going to access the online environment. Schools cannot regulate this environment completely – mobile phone access now competes with computer access in the school playground and increasingly in the classroom. Students are out of school more hours than they are in school so their access continues to expand.

Appropriate controls and filtering will minimise the risk:-

- Community education on identity theft and privacy breaches needs to keep pace with the development of these practices.
- Government is well placed to monitor developments and develop community education programs to address these issues.
- Education of parents on minimising the risks is essential to reduce the risk to children and young people.

Because the school computer environment is filtered, the risks are minimised in that environment. However, increased use of mobile phones with open access to social networking sites has increased that risk. In addition, students will bring to the school environment experiences from the home environment.

One of the greatest risks to young people is the permanence of the postings made on the internet. This concept is not fully understood by Gen Y and Gen Z. Government needs to consider protections to reduce the permanence of postings for under 18s.

The NSW SPC:-

- agrees that teachers are in a unique position to influence the understanding of students about the risks in the online environment but teachers do not have the most current information and given the already crowded curriculum it would be inappropriate for this to become *an addition* to the mandated Australian curriculum without a corresponding reduction. A more positive way to support our young people in the development of the skills required to deal with cyber-issues would be to include, *as part of* the PDHPE curriculum, at all stages:- development of resilience, understanding of, identifying and dealing with conflict, developing a range of communication skills including interpersonal skills. Cyber issues education needs to begin in Primary schools and is consolidated in secondary education.

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

Government needs to develop international-Australian agreements so that international & Australian sites that cause issues for young people can be forced to remove inappropriate material that constitutes cyber-bullying, illegal content, content which encourages inappropriate social or health behaviours or content that can lead to identity theft.

Governments need to develop international-Australian agreements so that international & Australian sites are required to remove material that can cause long term issues, uploaded by persons under 18years of age. Legislative support would make this easier to address.

Government has a role in identifying safe practices and providing guidelines to providers to maximise the likelihood that safe practices will be implemented. These guidelines need to be applied to all providers in Australia.

It does not appear that appropriate legislation is in place to allow police to demand that material causing offence to individuals be removed from the internet. Inter-government agreements would need to be reached as many websites that young people have difficulty with are based overseas. Websites could be banned from accepting anonymous postings – as a first step.

The issue of who judges and has removed inappropriate content is much broader and would likely require a separate inquiry to decide what was inappropriate and to whom. Having said this there do need to be some increased protections for under 18s. Perhaps parents could register a mobile phone as a 'teen phone' and then automatically get some filters attached to the phone plan that parents have the right to administer.

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

Creation of international-Australian communication agreements would allow management of inappropriate sites and removal of harmful and inappropriate content.

There is wide recognition that there has been a significant increase in time spent by Senior Executive and Welfare Officers in schools in dealing with cyber-safety issues. It is not appropriate that schools spend such a significant resource dealing with out of hours communications that lead to student-student conflict or family conflict nor should this be the sole responsibility of the school.

Cyber-harassment of staff should also be recognised when considering the importance of stakeholders working together. The anonymity of some sites does allow staff or schools to be the targets of inappropriate content. Tracing of the source of the postings would be helpful in preventing these postings in the first place.

One of the biggest frustrations identified by Principals is the inability to trace the sources of cyber-bullying where that bullying has a direct impact in the school environment. Compounding this the inability, even with police support, for schools to have removed from these websites harmful and inappropriate content.

If government could legislate to ensure this removal can occur within Australian sites and negotiate with international governments for similar actions for overseas sites follow-up in schools would be significantly easier and more effective.

- (v) Examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised.

Ensuring that schools can do their business in an effective and economic manner needs to be considered. There are times when the technology means that parents are on the doorstep before the school personnel are even aware there is an issue. Since this is happening in schools it is likely this practice will extend into the business arena. Mark Pesce identified this as “helicopter parenting” – a practice he says is prevalent in USA.

There are real learning benefits attained through the use of technology. To maximise the benefits and minimise the risks schools need government to support the school environment in a number of ways including but not limited to:-

- Developing parental responsibilities for access, management and use of technologies in the wider environment
- Ensuring staff in schools have access to current technologies and current information about what can be achieved using these technologies
- Inclusion of the use of technology as a teaching strategy available to teachers when leading learning for students rather than mandating the use of specific technologies
- Developing international-Australian agreements and guidelines to manage inappropriate content and practices
- Providing guidelines for Mobile Phone and Internet providers, including specific targeting of under 18s for more increased safety.
- Maintaining a web presence with valuable cyber-safety focus for young people, parents and the community.

- (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

International-Australian agreements that allow for removal of harmful and damaging content from overseas websites will improve capacity of those dealing with cyber-bullying to respond to that situation. Without this capacity schools will never be fully effective in dealing with cyber-safety.

The fundamental responsibility cannot fall to the schools. Values underpin the decisions to use the internet for cyber-bullying. Training needs to start with the very young at home. To start with teenagers may be too late. Parenting supports need to help parents develop safe cyber practices at home. In addition to Australian Curriculum and other priorities, schools cannot address cyber-safety as well without reduction elsewhere in an already overcrowded curriculum. It is essential adequate resources are provided to ensure teacher’s professional development keeps pace with changing technologies.

Schools need to continue to emphasise their culture of 'respect' and 'responsibility' to reduce the incidence and harmful effects of cyber-bullying. Schools and our system already run effective anti-bullying programs however these programs could be improved by a mechanism for sharing wise practice – across Kindergarten to Year 12. These programs need to be resourced and recognised as a valued part of the curriculum and not an “add-on” if schools are going to be expected to take the lead on educating young people on cyber-safety.

NSWDET has a unique opportunity to develop and include a cyber-safety program as part of the rollout of DER Notebooks. NSW DET has embarked on development of such a program which includes information for student online access on the following domains:- Digital Conduct, Digital Footprint, Digital Relationships, Digital Health and Wellbeing, Digital Law and Digital Financial Literacy. Parent awareness will be raised at the parent meetings prior to issue of the DER Notebooks. It is because this issue has already been addressed that NSW DET is in the position to further educate the community.

[\(vii\) Analysing information on achieving and continuing world's best practice safeguards](#)

NSW SPC has an expertise in analysing information and identifying best practice. For specific response see section (vi) as above.

[b\) such other matters relating to cyber-safety referred by the minister for Broadband, Communications and the digital Economy or either House.](#)

There are some fundamental questions this inquiry could answer that would assist schools in dealing with instances of cyber-bullying that affect schools. These include:-

- A clear legal definition of 'cyber-bullying'.
- Consistent State and Federal legislation.
- Provide guidelines regarding the actual legislation governing cyber-bullying and how it affects young people.

Government could commission some research into the links between increased adolescent mental health and the silence and anonymity of mobile phone and social website use. This would potentially inform key stakeholders and assist in the management of this demanding arena of Health that affects schooling and society.

This inquiry provides an opportunity for policy makers, parents, employers, the media and schools to work together to eradicate all forms of bullying, including cyber bullying.

Tracy Provest
Executive Member - Technology Portfolio.
on behalf of
NSW Secondary Principals' Council.

c/- Tracy Provest.
Principal.
Ulladulla High School.
Camden St, Ulladulla. 2539.

