SUBMISSION No. 11



Australian Education Union

Submission

to the

Joint Select Committee on Cyber-Safety

June 2010

Angelo Gavrielatos Federal President

Susan Hopgood Federal Secretary Australian Education Union Ground Floor 120 Clarendon Street Southbank VIC 3006

 Telephone:
 +61 (0)3 9693 1800

 Facsimile:
 +61 (0)3 9693 1805

 Web:
 www.aeufederal.org.au

 E-mail:
 aeu@aeufederal.org.au

Australian Education Union Submission to the Joint Select Committee on Cyber-Safety

1. <u>Introduction</u>

The Australian Education Union (AEU) represents 180,000 teachers, educators and support staff in the primary, secondary, TAFE and early childhood sectors throughout Australia. The AEU welcomes the opportunity to comment on matters of cyber-safety and unsociable behaviours that are affecting the health and wellbeing of young people in Australia.

The Inquiry is concerned primarily with online risks and challenges faced by Australian children, responding to the rise in community concern for matters including:

- the increased use and dependence on mobile phones;
- using mobile phones to capture violent assaults for distribution/publication; internet use which publishes and exposes social lives via social networking sites (including the broadcast of personal details and photos);
- use of personal websites, blogs, social networking communities, chat rooms, instant messaging and gaming websites to harass and bully;
- the existence and promotion of unsociable behaviours online including sexual content, access to pornography and violent imagery, risky behaviours such as underage drinking, smoking, drugs, gambling and the promotion of an unrealistic body image;
- identity theft; and
- technology addiction.

The AEU shares this concern particularly as young people's technology use overlaps their educational experience and now so too does the negative implications. While some of these implications of the extent to which students' personal lives are no longer private are not new to schools and educators, the prevalence of technology in everyday life appears to have escalated students' experiences of bullying, violence, harassment and crime.

As a concept, the AEU acknowledges that cyber bullying of students and teachers/administrators is on the rise and we therefore require a more effective response from parents, schools, authorities and providers, to keeping up with the pace of technological change.

The AEU views the issue of cyber-safety as a whole-of-community issue, not just the responsibility of schools to address. At the core of the problem is disrespectful behavior, not the medium by which individuals carry out the bullying. Too often, the media reports cyber-bullying incidents or inappropriate use of social networking as if it's technology itself to blame instead of the person using it.

The *Bullying*. *No Way!* website says "bullying is usually defined as any offensive or aggressive behaviour directed at another person, repeated over time. It may be physical, emotional or social. Cyber bullying, as it has become known, includes text or images posted on personal websites or transmitted via email or cell phones."

The consequences of cyber bullying are just as real, except that there is a perception of invisibility online and that therefore perpetrators don't realize that people still get hurt. Bullying in any form can result in long-term psychological harm such as low self-esteem, depression, anger, poor academic performance, truancy, and, in some cases, violence against self or others.

Cyber bullying, as opposed to bullying experienced by young people of previous generations (which mostly ended at the school gate), is now all pervasive due to the 24/7 reality of the internet and communication technologies.

Psychologist and teacher Marilyn Campbell (2009) from the University of Queensland explains that the complication with cyber bullying is that not only do students feel humiliated telling an adult but particularly as "most adults don't know that they have a cyber life – and if they then report the technology will be taken away from them." This obviously makes monitoring and prevention of cyber bullying incredibly complicated for Governments, education systems and educators.

Whilst much of the examples used in this submission are concerned with bullying aspects of cyber-safety, the AEU is just as concerned that education and support programs build resilience against anti-social behaviours facilitated via online technologies such as the sexualisation of children, access to pornography and violent imagery, risky behaviours (underage drinking, smoking, drugs, gambling) and the promotion of unrealistic body image.

Without detailing the gamut of negative impacts such behaviour can elicit, the AEU has standing policy - "*Standing with the Young 2000*" and "*Gender Equity Policy 2006*" - which acknowledges that young women and men negotiate an increasingly difficult pathway to adulthood. In terms of the pressures and access to information promoting risky behaviours, there may be gendered differences, but these certainly contribute to unhealthy relationships between young people which are equally disturbing (and preventable with adequate education and support).

Indeed, Maggie Hamilton argues in her article "*How we are screwing up boys with violence, porn, drugs and alcohol*" that when you then add in the "challenges of cyber-bullying, increased levels of violence in games and in the playground, the pressure to look a certain way, act out, concerns around body image, the pressure to drink and how to operate in an increasingly sexualised environment, you begin to realise this is a lot for any kid to deal with especially when parents aren't up to speed."

For girls, the repercussions of boys' level of online exposure, (to not understate their own pressures regarding body image and sexuality) are dire. Hamilton's observations should be seriously considered in the context of anti-violence strategies as studies show that "repeated exposure to porn shuts down a boy's feelings, and may even lead him to become a sexual abuser."

Similarly, Professor of sociology and women's studies at Boston's Wheelock College and author of "*Pornland: How porn has hijacked our sexuality*" Dr. Gail Dines, vehemently opposes the consumption of pornography for its construction of unrealistic sexual experiences. She argues (2010) porn promotes "a sex that is debased, dehumanized, formulaic and generic, a sex based not on individual fantasy, play or imagination, but one that is the result of an industrial product created by (mostly) men who get excited, not by bodily contact, but by market penetration and profits. A sex that encodes deep cultural scripts of male entitlement and female subservience."

As the AEU Gender Equity policy states, there is a great need therefore for health and human relationships education and resilience programs to empower young people in terms of boundaries and respect in relationships and overall to guard against self harm, harm of others and unhealthy/abusive future relationships.

However, the AEU wishes to also draw the Inquiry's attention to the experiences of teachers resulting from the saturation exposure of their professional and personal lives (which become increasingly compromised) to the online community.

The AEU will therefore respond broadly to the terms of reference in this submission, rather than on an item by item basis.

2. <u>Mitigating the Worst of Technology</u>

The AEU believes that as most responses to cyber safety have an element of 'trial and error' about them due to the relative newness of the technologies posing social concerns, but that these initiatives nevertheless have the best of intentions. So too have the efforts of private online companies' responses to a growing community sense of urgency to act due to tragic incidents, demonstrating the complexity of how online material should be treated.

The urgency for action is prompted by such horrific situations such as the suicides of teenagers (Sydney's Alex Wildman in 2008 and four Geelong teens in 2009) and the murder this year of Nona Belomesoff after befriending a man on *Facebook*.

There is a growing awareness that social networking sites' like, *MySpace* and *Facebook*, are alarmingly being used as vehicle for bullying and predatory/stalking behaviour.

Sadly, the flaws and potential for misuse (when users are naive to the level/extent of personal information being potentially broadcast via these sites), of social networking sites like *Facebook*, were revealed through tragedy.

Students, educators and parents need to be aware of the reality of their profiles and extent of broadcast such sites have the capacity for without users' direct choice. For example its more often a default setting for profiles to be 'searchable' to all internet users and this includes name, location, friends, photos, etc. Further, "friends" often have the ability to post personal information/photos or commentary about another person to all internet users without that person's expressed permission.

Police are at pains therefore to reinforce the message that just like prior to the era of online social networking, people shouldn't talk to strangers – that is to not treat people met online as 'friends'.

For teenagers particularly there is a danger of displaying, and frequently changing, their "relationship" status as there is an obvious danger for a young girl or boy to be displaying that they are single to potentially everyone on the internet.

As a result of pressure, *Facebook*, has made changes to their privacy settings so that a level of security can be applied to all areas in one click, or allow the user to customarily apply security measures depending on their preferences. However less information will now be automatically public, like hometown or hobbies/interests, and changes made will apply retroactively as well as for new services. Importantly, *Facebook* will stop updating its privacy settings so frequently to avoid confusion and makes users less vigilant.

Another policy response to note, this time by the Federal Government, is the controversial clean feed censoring proposed for Internet Service Providers in Australia, (or named the "mandatory ISP-level filtering of Refused Classification rated content" policy).

With the intention to restrict the distribution and publication of child sexual abuse material in particular, and consequently to prohibit children being exposed to such content online, there remains concerns that the policy's aims cannot be best satisfied through censorship and that instead legal subject matter will suffer undue restrictions.

Opponents of the clean feed recommend parents themselves install voluntary filters which are readily available which offers them greater control of what content they do not wish their children to be exposed to and that police resources should be increased to continue to infiltrate and prosecute groups of people responsible for creating and distributing such offensive and illegal material.

Parents do need to take much greater responsibility for the provision and use of technology by their kids. They need more information and education, as do teachers, youth workers, community agencies and anyone else working with children and young people.

In schools, unsophisticated forms of filtering can often get in the way of being able to use the internet for teaching and learning, e.g. not being able to look up sexual reproduction, or sex-linked genes because it has the word "sex" in it. The two examples mentioned here serve to highlight the intricacies of internet possibilities and how, due to its reach, information distribution via technology is so difficult to contain.

There are some in the community who therefore argue the merit of introducing an online ombudsman who has the power to investigate, advocate and act against illegal and inappropriate online content.

Recommendation 1:

The AEU would be supportive of a feasibility study into the role, powers and objectives of an online ombudsman in preference to a mandatory ISP-level filtering policy.

3. Digital Literacy and the Curriculum

The Federal Government's "Digital Education Revolution" has supplied computers to all Year 9 to 12 students. States/territories have also been provided additional money for maintenance and professional learning, some of which must go toward supporting teachers to educate students about the safe and ethical use of technology.

Further, in order to maximize opportunities and economic benefits of new technologies, educators must engage their students in online and digital learning.

The use of ICTs in the curriculum is an essential tool to enable students to fully participate in the rapidly changing digital world. Communication, commerce and democracy all have growing technology uses. Educators want and must ensure digital literacy remains central to the school environment, however we acknowledge that with this participation comes risk and responsibility.

The National Curriculum must integrate responsible and ethical use of ICT, respectful relationships, and protective behaviours etc. The implementation of the National Curriculum clearly requires additional funding anticipated for teacher professional learning around planning and delivery.

The AEU acknowledges that students often engage in online activity without knowledge of parents/adults so we must be teaching students resilience and protective behaviours.

The AEU therefore wholly supports the approach advocated by the *Bullying*. *No Way!* website, which recognises that "cyber bullying occurs in on-line environments where there are no responsible adults present therefore it is important that young people are taught to independently prevent cyber bullying and to address the underlying issues. Curriculum programs incorporating social skills and values education as well as direct teaching of "nettiquette" could all help to reduce cyber bullying. Peer helper programs, buddy programs and transition programs will also help to develop an ethos of support in the school community."

For example, the AEU welcomes Victoria's cyber safety sessions which were held in 27 schools for the first time in early June this year as part of a series of age appropriate awareness and prevention programs.

The programs involve year 3 and 4 students discussing what being cyber smart means to them on a SuperClubs Plus closed chat site. Students in Years 5 to 10 participated in an online video session where they discussed what cyber bullying is, what it means and what students can do about it. And they also then conducted cyber safety research in their schools before reconvening for another online conference with their student group and cyber expert later that month.

The AEU, like many organisations, advocates a whole school approach and for well communicated procedures. Policies related to internet use, cell phone use, bullying, and suicide prevention should be reviewed to address:

- Code of conduct for use of technology.
- Effective supervision and monitoring for deterring cyber bullying.
- Effective intervention for detecting, investigating, and responding to incidents of cyber bullying.
- Reporting of cyber bullying.

Ideally, such responses should involve over-arching system policies which schools can then supplement with more detailed procedures.

But there is a need to support students once bullying or another online incident occurs and in this sense it is crucial that a culture of reporting (including clear processes for when Police must become involved) be cultivated in schools and the community more broadly. There are even suggestions about possible ways to encourage reporting, like via SMS, email, phone line or chat room, which utilise the ease of technologies themselves are worth pursuing.

The NSW Coroner recently recommended that the numbers and resources for school counsellors be drastically increased to help support the increasing social welfare needs of students which the AEU wholly agrees with.

Many schools don't have full-time professionally qualified counselors and some schools students can only access a counselor for half a day per week. The AEU is aware that training, recruitment and retention of counselors is a significant problem across the country in all school sectors.

Further, any increased effort around supporting students should rightly advocate that all staff participate in professional development in general awareness in ways to detect, review and intervene.

Recommendation 2:

The AEU supports the NSW Coroner's calls for the numbers and resources for school counsellors be drastically increased to help support the increasing social welfare needs of students arising from their cyber engagement.

4. <u>Government Programs</u>

Given the timing of this Inquiry has coincided with the National Cyber Security Awareness Week there are a number of initiatives being promoted that warrant comment.

The Federal Government's "Budd:*e*" cyber security education modules (primary and secondary) should be recognised as comprehensive and well worth the profession's support.

Further, the Australian Communication and Media Authority's (ACMA) 'Cybersafety Outreach - Pre-service Teacher' training program is also the sort of approach to supporting educators that is required.

Specifically the program equips pre-service teachers with the skills and knowledge to educate their future students about cyber safety issues such as cyberbullying, sexting, safe social networking, e-security and identity protection. It also goes to the heart of responsible digital citizenship, providing an appreciation of some of the ethical issues involved.

The ACMA is to be commended for their age-appropriate program for students, plus sessions for parents and importantly also provides similar professional development for practicing teachers which encourages a comprehensive understanding of a modern student's technology profile, digital literacy, positive online behaviour, personal and peer safety and the school's and teachers' legal obligations to minimise and address risks.

The Federal Government's *Cybersmart* website lists national, state and territory cybersafety policies including the "*Better Practice Guide: ICT in Schools*" which provides guidance for ICT use and the "*National Safe Schools Framework*" developed the Ministerial Council on Education, Employment, Training and Youth Affairs (MCEETYA) which is currently undergoing a review.

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

It rings true that 'it takes a village to raise a child' however there is concern amongst educators that schools alone will be held responsible for the online activities of children and young people. This fails to take account of the broader societal responsibility that exists, to support children and young people to develop responsible, safe, respectful behaviours in all aspects of their lives. The Attorney-General's "*Protecting Yourself Online – What Everyone Needs to Know*" booklet which has information for adults about their digital security but also ways to monitor and mitigate the dangers of their children's online/technology use provides an important cross over between the cyber safety concerns for all technology users as well as active engagement as adults.

As adults the AEU would encourage community members to take the advice of *Bullying*. *No Way!* (but not only regarding bullying) and consider the following action:

• Get involved and be aware

- Learn everything you can about information and communication technologies and how your child is using them. Talk to them about the places they go online and the activities that they are involved in.
- Encourage your child to come to you if anybody says or does something that makes them feel uncomfortable or threatened. Stay calm and keep the lines of communication and trust open. If you "freak out" they won't turn to you for help when they need it.

• Take action if your daughter or son is being bullied online

- Watch out for signs that your child is being bullied online a reluctance to use the computer or go to school may be an indication.
- If the bullying is coming from a student at the same school, meet with school officials and ask for help in resolving the situation.
- Report any incident of online harassment and physical threats to your local police and your Internet Service Provider (ISP).
- If your child is bullied through a mobile phone, report the problem to your phone service provider. If it's a persistent problem you can change the phone number.

• Encourage your child to develop their own moral code so they will *choose* to behave ethically with the technologies

- Talk to them about responsible use. Teach them to never post or say anything that they wouldn't want the whole world including you to see or read.
- Work with them to create a contract or agreement with clear rules about ethical behaviour.

Recommendation 3:

Staff professional development must be offered (and fully funded), in general awareness in ways to detect, review and intervene in cyber-safety matters.

Recommendation 4:

Any policies to increase education and awareness on cybersafety within schooling should be on a systemic/whole school basis where over-arching system policies exists and supplemented by schools with their own more detailed and well communicated procedures.

Recommendation 5:

The AEU commends government efforts to date about cyber safety issues such as cyberbullying, sexting, safe social networking, e-security and identity protection but encourages greater inter-agency collaboration and broader community engagement in prevention strategies.

5. <u>Teacher Privacy, Professionalism and Legal Responsibilities</u>

The final matter the AEU would like to bring to the attention of the Select Committee is our growing concern for and evidence of teachers professional and personal lives becoming increasingly compromised by digital technology.

The union is regularly contacted by members who are experiencing personal and professional attacks via internet sites such as "Rate My Teacher", *Facebook*, and *MySpace*. We have allegations brought to our attention of students filming teachers' classes on their mobile phones and uploading videos onto YouTube with disparaging comments.

This Inquiry and the community need to clearly understand that many forms of cyberbullying amount to criminal behavior. Whether toward young people or their educators (and support staff), schools and education systems have a legal liability to act to prevent criminal behaviour and most importantly to collaborate with police when incidents occur.

There continues to be ethical and legal concerns with educators' online presence which blur the teacher/student relationship – for example when students seek to be "friends" with teachers on *Facebook*.

Further, the questions surrounding extended or unclear Duty of Care responsibilities weigh heavily on our members. As has been the case with remote education and now with a move towards a Virtual Learning Environment (VLE) - where there can be online video lessons (viewed by parents as well), homework, teacher resources etc - the challenge posed is "what is a class?" When students may be scattered across the state/territory they are in, or even several states, the notion of duty of care is vexed. Without standard face to face teaching hours, there are huge implications for the workload of a teacher when students and parents could have 24 hour access to teachers via email, etc.

The AEU through its Branches and Associated Bodies are attempting to develop responses to these concerns to protect our members' cyber safety as much as that of our students.

For example, in South Australia there is a Coalition to Decrease Bullying, Harassment and Violence in SA Schools which comprises the 3 main education authorities, (DECS, Catholic Ed and Independent Schools) together with the University of SA. This coalition has produced brochures for families etc on Cyber bullying, ecrime and the protection of children and young people.

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

However we believe that this effort should not be constrained to the role of the union but for education departments, as the employer, to broaden their cyber safety policy responses to recognise the needs of the profession also.

Education systems must negotiate with the profession, through their unions, any introduction of new technologies into schools and systems, fully examine workload and safety implications before implementation.

Recommendation 6:

The AEU encourages education systems to continue to engage the education profession in professional learning about both rights and curriculum support to responsibly teach online learning/digital literacy and citizenship. Such opportunities need to be fully funded and accessible to practicing teachers and pre-service teachers.

Recommendation 7:

Education systems must work collaboratively with the Police in regard to criminal behaviour whether it is face to face or via technology. Education systems, as the employer, must broaden their cyber safety policy responses to recognise the professional, ethical and legal needs of the profession also.

6. <u>Conclusion/Recommendations</u>

The AEU welcomes the concerted effort being shown by governments and the community to reduce risks and challenges faced by Australian children due to their technology use.

Attempts to customise privacy protection and to filter inappropriate online content is insufficient and fraught with unintended/undesired censorship.

When the use of ICTs in the curriculum is an essential tool to enable students to fully participate in the rapidly changing digital world, educators must be supported with the skills and knowledge to educate their future students about cyber safety issues such as cyberbullying, sexting, safe social networking, e-security and identity protection.

It is clear therefore that there is no shortage of effort going into policy responses to issues of cyber-safety but perhaps there is evidence of a need for greater inter-agency cooperation and for the a better engagement between schools and working within the broader community.

The AEU urges teacher privacy, professionalism and legal responsibilities be considered within the scope of this Inquiry and integrated into policy responses in the future.

Recommendation 1:

The AEU would be supportive of a feasibility study into the role, powers and objectives of an online ombudsman in preference to a mandatory ISP-level filtering policy.

Recommendation 2:

The AEU supports the NSW Coroner's calls for the numbers and resources for school counsellors be drastically increased to help support the increasing social welfare needs of students arising from their cyber engagement.

Recommendation 3:

Staff professional development must be offered in general awareness in ways to detect, review and intervene in cyber-safety matters.

Recommendation 4:

Any policies to increase education and awareness on cybersafety within schooling should be on a systemic/whole school basis where over-arching system policies exists and supplemented by schools with their own more detailed and well communicated procedures.

Recommendation 5:

The AEU **c**ommends government efforts to date about cyber safety issues such as cyberbullying, sexting, safe social networking, e-security and identity protection but encourages greater inter-agency collaboration and broader community engagement in prevention strategies.

Recommendation 6:

The AEU encourages education systems to continue to engage the education profession in professional learning about both rights and curriculum support to responsibly teach online learning/digital literacy and citizenship. Such opportunities need to be fully funded and accessible to practicing teachers and pre-service teachers.

Recommendation 7:

Education systems must work collaboratively with the Police in regard to criminal behaviour whether it is face to face or via technology. Education systems, as the employer, must broaden their cyber safety policy responses to recognise the professional, ethical and legal needs of the profession also.

References

Campbell, M., (2009), "*What are young people saying about cyber bullying?*", published on <u>http://www.bullyingnoway.com.au/talkout/profiles/researchers/marilynCampbell.shtml</u>

Hamilton, M., (2010), "How we are screwing up boys with violence, porn, drugs and alcohol", published, June 2nd on <u>http://melindatankardreist.com/</u>

Dines, Dr., (2010), "*Opposed to porn sex: debased, dehumanised, formulaic and generic*" published, June 22nd on <u>http://melindatankardreist.com/</u>