Australian Secondary Principal's Association

Submission: Inquiry into Cyber-Safety

Introduction

The Australian Secondary Principal's Association is the peak body representing Secondary Principals in government schools across the country. Government schools, by far, provide educational services to the largest number of secondary aged students in this country.

Our submission will outline key issues impacting on secondary schools and recommend ways schools can be supported in helping society address this social problem.

Context

The misuse of mobile phones, social networking media, email and other Internet or electronic devices to harass, bully, abuse and threaten the safety of young people has increased significantly in high schools and the wider community over recent years. The level of youth involvement in this area is concerning to Secondary School Principals. This type of crime has serious short-term and long-term effects on the physical and mental health of our young people.

A number of educational jurisdictions across the country have recognised this as a major social issue confronting our young people and commenced programs and strategies to address this abuse of what is essentially a beneficial technology.

Virtually all schools across all sectors of education will have students who have experienced cyber-safety issues. Unfortunately, secondary school aged young people appear to be those most vulnerable with different levels of severity and frequency. The influence of cyber-crime can be multi-dimensional resulting in isolation, fear and even lead to violence.

Technology is accessible 24 hours a day, seven days a week and that means that our young people are more vulnerable outside school hours. It also means that they are connected into a medium that takes them out of their local community and into

the multiple time zones and diversity of the global community. While the majority of our young people use technology responsibly, it's important that everyone is alert to the potential for harm and to know where to find help and support.

Secondary schools can only be part of the solution, but a very important part. Therefore, it is important that any educational initiative include a cooperative effort with other agencies, families and individual members of society.

Current Practice and Issues
Educational authorities have introduced many state-based and school-based internet/cyber-safety agreements for students as well as filtering systems on internet access for email and websites.

Schools endeavour to create and maintain a cyber-safety culture and use agreements to outline student's obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment. Parents have also been encouraged to join efforts to reduce the incidence of cyber bullying, harassment and improve cyber-safety.

Using ICT's responsibly and ethically is part of everyday practice in secondary schools. Students learn about internet safety, digital reputation, cyber-bullying, what is appropriate and what is not appropriate for online communication. Student work is generally monitored closely by staff to ensure safety and privacy is protected.

While every reasonable effort is made by a school or system to prevent student exposure to inappropriate content, it is impossible to completely eliminate the risk with the amount of time students are spending online outside school hours. Principals in Secondary Schools have significant concerns regarding the amount of time that some of our young people are online at night and the impact on their ability to concentrate on their education.

Support for Schools and Young People
Our primary focus in schools is education and the development of our young people to live productive lives that contribute to society as a whole.

We believe Schools do have a role to play in educating our young people about cyber-safety; however, that role must be balanced in the context of the main purposes of schooling, the role parents play and the responsibility of society in general.

Throughout our government schooling system, schools already contribute significantly to the cyber-safety education agenda at various levels within the curriculum.

Schools provide a very safe environment for our young people and safety is instilled into school culture, however, there are always processes that can be improved to provide greater protection.

The role schools play in the delivery of cyber-safety education must not be increased beyond what time is already allocated. The curriculum is overcrowded by demands from all levels of society and interest groups. To simply add additional information that must be passed on is not possible without removing other content from the current curriculum.

Principals and teachers are not experts in cyber-safety, but they play an important role in conveying the message due to the relationship they have with the young people they teach. Teachers know how to convey the message appropriately and take into account individual student needs and learning abilities. Staff need specific training to deliver any material that is expected to be taught at the secondary school level. Furthermore, to deliver this message appropriately, it must be fully funded and resourced. Materials and instructional processes used for cyber-safety education in schools must be well researched, clear and promote positive social norms.

There are many programs and initiatives (Kids Helpline, Alanna and Madeline Foundation, ThinkUknow, ACMA, etc) already available to young people and families. It is important that resources such as these have evidenced-based information, are evaluated and accredited before being broadly introduced into all schools or the community. We need to understand why young people become victims and why these events occur. We need to find out which components of which programs are most effective in various circumstances and how these strategies and programs can be improved.

There is currently an absence of systemic and ongoing survey data from this context, showing trends, successfulness of intervention programs, victim restoration and perpetrator rehabilitation. A shift in approach is needed to uncover the size and dimensions of the problem and how it changes over time. Such research will inform and direct prevention strategies.

It is currently impossible to state with any confidence the level of student engagement in cyber-crime as comprehensive data is non-existent.

Schools need access to reliable data and web-based resources that are regularly updated to contend with the constantly changing cyber-safety environment.

Parenting strategies, including parental monitoring of young people needs improving. Society has a responsibility to educate parents on how to monitor and educate their children in cyber-safety.

Other Considerations

Corporations and individuals who develop programs for use in this technology rich environment (Google, Facebook, etc) also have social responsibilities for the safety of our young people. To say that all members of society should be able to have open access to any material or pathways through the internet or communication channels, is neglecting that responsibility to raise our children in a caring and safe environment. These programs need to provide parents and our young people with warnings, restriction options and help options if needed.

Concluding Comments

As professionals, who invest daily into the education of our young people, we believe any approach must be consistent across the country and based on good research. Implementation needs to be well planned, resourced at a level that will enable success, viewed as a cooperative effort with families and society in general.

Recommendations

1. That an explicit and consistent approach to cyber-safety be implemented across Australia for parents and educational institutions.

2. That programs and strategies implemented are evidence-based, founded in internationally benchmarked research and resourced at an appropriate level to ensure success.

3. That the federal government, through its agencies provide a web-based, one-stop-shop of resources for schools to use.

4. That a longitudinal study be undertaken into the use and abuse of these technologies to gather data and inform future policy and procedures associated with this scourge.

5. That a system of evaluating and accrediting cyber-safety programs be set up.

6. That corporations and individuals who develop social networking media be held accountable for monitoring their sites and immediately removing material that breaches a code for cyber-safety.

Submitted by Norm Fuller on behalf of ASPA. Ph:0408786529; email: nfull6@eq.edu.au