AEU Tasmanian Branch Submission to the Joint Select Committee on Cyber Safety

The Australian Education Union (AEU), Tasmania Branch, welcomes the opportunity to make submission to the Joint Select Committee on Cyber Safety. The AEU Tasmanian Branch represents the industrial and professional interests of more than 6,000 educators in Tasmanian government schools. In Tasmania, more than 70 per cent of children attend public schools and the AEU is the largest organisation lobbying for improvements to that sector of education.

Introduction

Developments in information and communications technology and cyberspace are rapid. Access to the internet now extends to mobile phones and, through access to these and with 72 per cent of Australian households having internet access, many children have relatively uncontrolled access to the internet. According to the current research literature, Australian teenagers continue to have access to ICT to a greater extent than their peers in many other countries and are among the highest users of ICT in the OECD. Evidence shows that the number of children aged under13 who use social networking sites and online gaming is growing.

These trends will only be enhanced by the Australian Government's creation of the National Broadband Network (NBN), which was launched in Tasmania, and the rollout of the Digital Education Revolution (DER).

In June 2008 the Ministerial Council for Employment, Education, Training and Youth Affairs (MCEETYA) declared, "Australia will have technology enriched learning environments that enable students to achieve high quality learning outcomes and productively contribute to our society and economy". There is clearly no reversing the move to greater reliance on ICT and indeed the nation's economic prosperity is linked to this to the extent to which it can embrace and effectively use such technologies.

The National Broadband Network, which began its rollout in Tasmania, whilst an essential move forward for the nations' ICT capacity may also compound the effects of cyber risk.

For children there are personal threats via cyber-bullying, online grooming, and sexting, or incidents of ID theft or fraud. There are matters relating to intellectual property. There are also – through less personal but more insidious – forms of threat to computers and systems such as spam attacks, phishing attacks, infected personal computers adding to botnets, distributed denial of service (DDOS) attacks etc. Matters of personal cyber security provide an impact on broader systems and even national security and Australia's digital economy. This potential risk has been foreseen by the Australian Government and acknowledged in statements by Communications and Digital Economy Minister, The Honourable Stephen Conway.

The online world is commonly part of children's daily environment both educationally and in their broader lives and, like the offline world, it has particular risks and ethical approaches which require learning appropriate knowledge and skills if children are to become successful and safe citizens within its realm. There can never be guarantees against malicious behaviour, but many risks which

are simply borne of ignorance can be significantly reduced if children are educated properly in the use of technologies.

In a similar way to educating children in a wide range of other matters concerning their health and welfare, an approach empowering them to make informed decisions has a strong underpinning of evidence for success. *Safer Children in a Digital World: The Report of the Byron Review (2008)*, recommended empowering children and young people to keep themselves safe online. The report contained Byron's oft-quoted analogy … 'at a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim'… In reference to the online world, the report proposed that there be warnings and filters, but that children must also be taught how to stay safe online. The report argued that trying to keep children from encountering potentially harmful material was pointless, because no matter how many safeguards are put in place individuals find ways to circumvent them.

In the United Kingdom, OFSTED inspections of schools now include audits of the schools programs for cyber safety education. The AEU does not see the educational offerings being improved through the introduction of an inspectorate, however resources need to be put into schools to ensure that teachers are able to provide appropriate programs of learning for children. The Department of Education, Employment and Workplace Relations (DEEWR) via the Digital Education Revolution, has concern for the digital literacy of children and young people and this matter is currently being addressed by the Australian Curriculum, Assessment and Reporting Authority (ACARA) in the development of Australia's new national school curriculum.

Given the nature and pervasiveness of the online world, in a context where warnings and filters have limited efficacy, the most effective approach to cyber safety is to build into classrooms good teaching and learning experiences. As well as excellent teaching and learning, effective partnerships between school and home must provide the best outcomes for young people in the online environment.

In order to provide an environment in which good practice is likely to flourish it is important that Governments and relevant authorities assist schools, through consultation, by developing appropriate standards which are understood and broadly agreed upon across business, government, education and broader community sectors.

Recommendations

The AEU sees that issues surrounding cyber-safety education cannot be separated from broader imperatives of digital literacy and sees this as a core component of the 21st century school curriculum.

1. To safeguard children and young people online, cyber-safety education needs to be provided for children and young people, their parents, carers and families, and their teachers and school staff. Schools must therefore be resourced to ensure cyber-safety education is built into core curriculum and properly supported.
2. To ensure quality and consistency across jurisdictions, educational standards for cyber-safety education need to be developed.

3. Standards need to be developed by the Australian Government for cyber-safeguarding, and the safe, responsible use of digital technologies. Such standards should prevail across all government departments and provide a beacon for the non-government sector.
4. To support students and educators, Education Authorities need to develop clear, consistent, system-wide policy guidelines and standards for cyber safety in schools.

References

Australian Curriculum, Assessment and Reporting Authority (2010). Draft Australian Curriculum Documents. At http://www.acara.edu.au/

Byron, (Prof) T. (2008). Safer Children in a Digital World: The Report of the Byron Review. Department for Children, Schools and Families. At http://www.dcsf.gov.uk/byronreview/

MCEETYA (2008). *Joint Ministerial Statement on Information and Communications Technologies in Australian Education and Training (2008-2011)*. At http://www.aictec.edu.au/aictec/go/home/about/pid/95