SUBMISSION No. 100

SUBMISSION TO THE JOINT SELECT COMMITTEE ON CYBER SAFETY

June 2010

CONTACT

Melinda Standish
Writer / Research
[redacted]

Craig Dow Sainter
Director
[redacted]

Roar Educate
www.roareducate.com.au

Roar Film Pty Ltd
www.roarfilm.com.au

Suite 340
Salamanca Arts Centre
77 Salamanca Place
Hobart
Tasmania
7000
T 03 6224 5222
F 03 6224 5511

roar educate
engageinteracteducate

INTRODUCTION

Roar Educate develops education software - exemplary e-learning for schools (K-12). Roar Educate is the education division of Roar Film Pty Ltd, the acclaimed Australian film and multimedia production company based in Tasmania.

Foremost Roar Educate is established in the UK, where the modules *Celebrating Us* and *Us Online* are already licensed to 43 per cent of English government schools (approximately 5 million students). *Us Online* (about internet safety and online ethics) was finalist at the prestigious 2009 BETT (British Education and Training Technology) Awards in London.

Also in 2009 Roar developed the *Budd:e e-security builder* under contract to the Australian Government (Department of Broadband, Communications and the Digital Economy). The two modules target primary school and secondary school students, and have been rolled out to every Australian school. *Budd:e e-security builder* won Best Children's interactive media at the 2010 AIMIA (Australian Interactive Media Industry Association) Awards.

Roar Educate has proposed the development of *Us Online Next Generation*, in partnership with the London Grid for Learning (LGfL, the high-speed broadband consortium serving London's 2,600 schools) and Catholic Network Australia (CAN, serving 1,550 Australian schools).

Us Online Next Generation is an online school-based system to promote digital citizenship and implement (in the digital space) the statutory duty to safeguard. *Us Online Next Generation* will enable the safe, ethical and responsible use of digital technologies by all parties across school communities… by students, teachers and staff, and parents.

Also currently Roar is working with the Australian Catholic University and the Wesley Institute to trial internationally competitive teacher education and continuing professional development about cyber safeguarding and risk management. Roar is in discussion with Prof Tanya Byron about the development of *Us Online Next Generation* and Roar's teacher professional development.

meme /meem/ *noun*. an idea or value or pattern of behaviour…

Are you being safe online? Is your stuff secure? Because this is 'the meme' for the online world.

Click on MENU for a SURVEY to see how far you go online, or to access the TEACHER CENTRE.

Choose from TV, WIKI or PLAY to find out more about your meme for the online world.

© 2009 | Roar Educate Ltd | roareducate.co.uk | Site Cr

We live in London, but the web puts the world at our fingertips.
Like the real world, the online world has good and bad in it, and going online is like going out in the real world.
We need to take care.

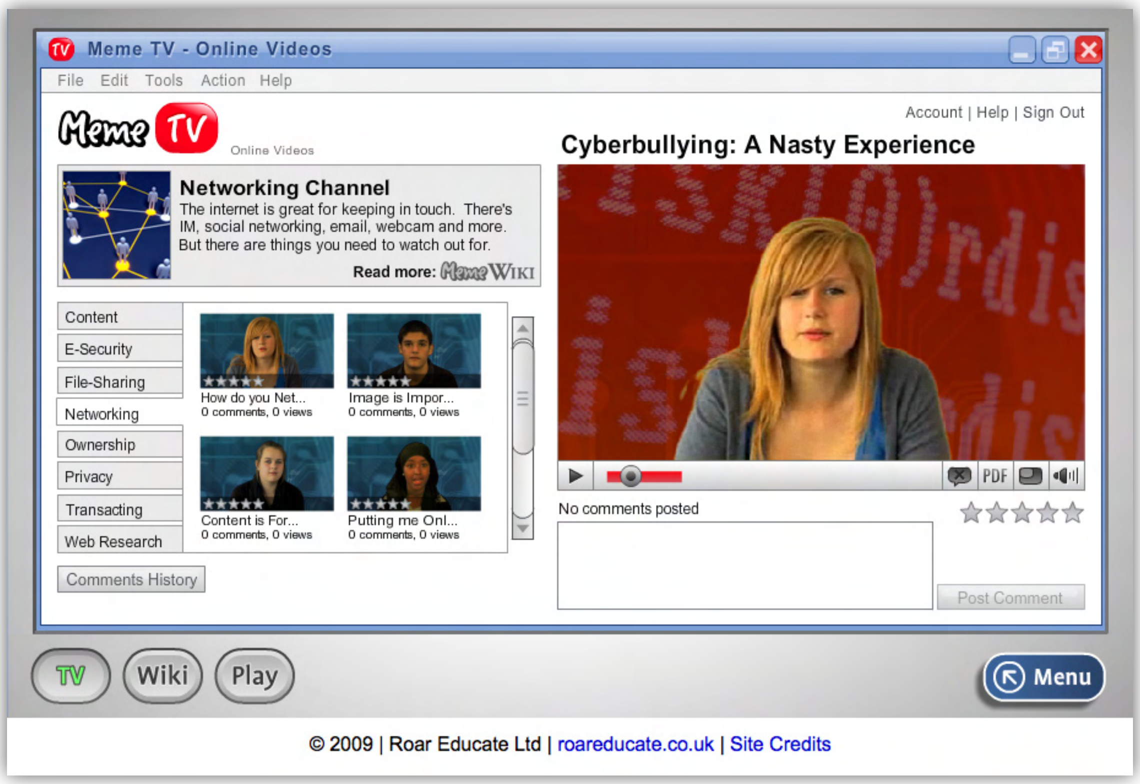
Here you'll find out about having a good, safe time online, and each activity unlocks another widget for your dashboard.

1 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)

Roar recognises the great speed of developments in the digital space. Particularly noted is the rapid uptake of Web 2.0 technologies by 'millenials', including webcam-based chat and location-based services, the use of internet-enabled mobiles and wifi-enabled portable media devices[1], as well as the growing participation of children aged under 13 on social networking sites[2], and online gaming.

According to the current research literature, Australian teenagers continue to have access to, and use, ICT to a greater extent than their peers in many other countries and are among the highest users of ICT in the OECD[3]. This trend will only be strengthened by Australian Government policy on two digital fronts, the creation of the National Broadband Network (NBN), 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".[4]



Cyberbullying: A Nasty Experience

Networking Channel

The internet is great for keeping in touch. There's IM, social networking, email, webcam and more. But there are things you need to watch out for.

Read more: Meme WIKI

No comments posted

© 2009 | Roar Educate Ltd | roareducate.co.uk | Site Credits

From Meme TV (Us Online for year 8 plus)

To realise the MCEETYA vision the Australian Government through the Digital Education Revolution – and in particular the National Secondary School Computer Fund – is investing $2.3 billion to provide for new or upgraded information and communications technology (ICT) for secondary schools with students in Years 9 to 12. The Fund aims to achieve a one-to-one computer to student ratio by the end of 2011. Already, 2,700 secondary schools across Australia have been approved for funding to purchase almost 290,000 new computers.[5]

Similarly, the NBN will have a significant impact on internet use by making available to users internet speeds up to 100Mb/sec. Already 72 per cent of Australian households have internet access, and 78 per cent have access to a computer. Three months ago the Minister for Communications (Senator Stephen Conroy) opened the Mornington proof of concept test centre and announced the first retail service providers who will work with NBN Tasmania to deliver the broadband services. In Tasmania (where Roar fortuitously is located) NBN is upon us.

The NBN is likely to compound the impact of developments because of the heightened levels of cyber risk: from serious threats to individuals via cyber-bullying, online grooming, and sexting, or incidents of ID theft or fraud, or matters relating to intellectual property, through to less personal but more insidious forms of cyber-threat including spam attacks, phishing attacks, compromised personal computers adding to botnets, distributed denial of service (DDOS) attacks etc - matters of personal security that directly impact on national security and Australia's digital economy.

Anticipating NBN, in May 2008 Senator Conroy stated, "With the development and rollout of Labor's national broadband scheme, we expect that there will be an increased opportunity for bad behaviour … so it's very important that we try and not wait till the horse has bolted".[6]

No question, it is in the national interest that Australians embrace the digital space, particularly all that Web 2.0 offers. But cyber risks are many to a high-speed internet-enabled society. Do children and young people, parents and families - indeed all citizens – know how to make safe, ethical, responsible use of digital technologies? What are the mechanisms for cyber-safeguarding children and young people, and delivering current, dynamic cyber-safety education to the citizens of the nation?

[1] Department for Children, Schools and Families (2009), *Staying safe survey 2009*.
91 per cent of children and young people aged 12 to 17 (95 per cent females and 88 per cent males) have their own mobile phone and 12 per cent say they access the internet through their phone.

[2] Ofcom (2010), *UK children's media literacy: 2009 report* – found that one-in-four home internet users aged 8 to 12 said they had a page or profile on a social networking site which has a minimum user age of 13.

[3] MCEECDYA (2010). *National Assessment Program - ICT Literacy Years 6 & 10 Report 2008. Executive summary* at page xvi.

[4] 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

[5] See the National Secondary Schools Computer Fund, at http://www.deewr.gov.au

[6] 31 May 2008. *The Australian*. At http://www.news.com.au/story/0,23599,23787118-421,00.html

2 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 (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking);*
- *identity theft; and*
- *breaches of privacy*

Roar is broadly familiar with the current research literature, and monitors national, international and specialist technology and related media. In the context of developing education software, Roar works with focus-groups of children and young people, and undertakes user testing of Roar education content. We comment on the above anecdotally.

Undeniably all the above are risks associated with digital technology and the online world: 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 (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking); identity theft; and breaches of privacy

Sensationalist media reporting has tended to over-emphasise certain of the above risks, particularly cyber-stalking, sexual grooming and predation, and exposure to illegal (prohibited) content.

Two million internet addicts
Kate's Party gatecrashed by 60,000 Facebook users
TEENAGE GIRLS' PHONE HABIT HITS 100 MESSAGES A DAY
CALL TO RALLY AGAINST CYBER CRIME
YOUNG FACING ONLINE FRAUD RISKS
BOTNETS FORM 'BLACK CLOUD'

Young people typically view the online world as just another playground, and they fail to recognise critical differences from the offline world. They fail to recognise that some risks are elevated and escalated online: risks associated with the permanence of content, relative anonymity, the lack of an immediate consequence (for example, the facelessness of cyber-bullying), and issues that relate to the reach and spread of online communities. Other effects are noted including the speed of disclosure within online relationships, and what may be described as the 'disinhibition effect' that occurs for many young people on social networking sites.

Those most at risk online are the same group as those most at risk in the offline world: the same marginalised young people that turn up online as the victims of bullying, as the sexually-solicitous, or as proponents of racist or hate speech are typically the same groups as those at risk and marginalised in the offline world.

Risk-taking is a feature of adolescence, and for many young people the online world is an unsupervised, adult-free space.

Unsafe, unethical, and irresponsible use of digital technologies by young people may be purposeful and of malicious intent, but more often it will be due to bad advice or a product of ignorance.

Some of the greatest risks for children and young people come via their peers through acts like as cyber-bullying or sexting.

Cyber-risk is significantly reduced with education.

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

RESPONSE IN AUSTRALIA

Roar has formed the view that fear has been a major driver and shaper of the national response, supported by sensationalist media reporting of incidents: the abuse of children online, cyber-bullying, stalking or grooming, exposure to illegal and inappropriate content, technology addiction and related poor health outcomes, and so on. This has focused considerable attention on the negatives rather than the many positive benefits to education and life generally that come with safe, ethical and responsible use of digital technologies.

In the education sector, first instincts have been to 'lock down'. This has been the policy response across most industry sectors, but particularly in those with responsibility for minors. Within their sandbox environments, schools have been slow to encourage the use of Web 2.0 tools. Moreover, the sandbox seems to have obviated the need for engagement about cyber-safeguarding across school communities – between kids, teachers and parents.

In Australia cyber-safeguarding straddles the mega federal departments of Education, Employment and Workplace Relations (DEEWR), and Broadband, Communications and the Digital Economy (DBCDE). Cyber-safety also gets pulled across the federal-state divide, with responsibility for schools falling to individual state and territory education departments.

As yet there is no clear, national policy position on cyber-safeguarding for Australian schools. Australia's cyber-safety education response has been fragmented across government agencies and jurisdictions, and the various elements siloed:

- The Federal Government allocated $125.8 million for a national cyber-safety plan (including the proposed mandatory internet filter, and cyber-safety education activities). The bulk of allocated funds have gone to the Australian Communications and Media Authority (ACMA). As the broadcast industry regulator, ACMA was foremost concerned with the matter of illegal content, and illegal practices like online child exploitation. Today ACMA hosts an abundance of resources for educators and school administrators, but these do not constitute a systematic (or systems-based) approach to cyber-safeguarding and universal safe, ethical and responsible use of digital technologies.
- The Department of Broadband, Communications and the Digital Economy (DBCDE) is taking on the hackers, scammers and other threats to 'e-security'. Roar was contracted by DBCDE to develop stand-alone learning modules for Year 3 and Year 9 students, and last year the Budd:e E-Security Builder was rolled out to every Australian school. In November 2009 Mr Keith Besgrove reported to the House Standing Committee on Communications Inquiry into Cyber Crime that approximately 1,400 schools (of a possible 9,500) had accessed the online modules, but data was not provided regarding the level or nature of access[7].

[7] House of Representatives Standing Committee on Communications (June 2010). *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*. The Report of the Inquiry into Cyber Crime. Canberra. Pages 216-7.

Pick bits for your **Budd:e**. But for each part, you'll have to do an e-security challange.

To have a good time on the web, you need to keep yourself safe and make things e-secure—your computer, phone and other devices that you connect to the internet.

Here you'll find out about e-security—and you'll build your very own e-security **Budd:e**.

- The Alannah and Madeline Foundation (AMF) is concerned with violent or aggressive behaviour online: foremost cyber-bullying, but also sexual predation, accessing inappropriate content, being coerced into sending sexually suggestive images etc. The AMF Cybersafety and Wellbeing Initiative includes a National Pilot Program in Schools, to help confront safety issues in e-communications, particularly cyber-bullying.
- 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 will be addressed by Australia's new national school curriculum[8]. Indeed, skills and understanding for participation in new and emerging technologies will be a key feature of the proposed curriculum, but the articulation of digital literacy across the curriculum is some way off…

  ICT skills and understanding have been recognised as a 'general capability', together with 'ethical behaviour', 'intercultural understanding', and 'literacy' in relation to new media and digital technologies. But the new curriculum is yet to elaborate the ICT 'continuum' and define ICT achievement standards for Years 2, 6 and 10. These elements have been scheduled for the third phase of curriculum development. The first phase of curriculum development will run to late 2011, and the second phase has just commenced. The Australian Curriculum, Assessment and Reporting Authority has yet to advised timing for the third phase of development.

[8] See Australian Curriculum, Assessment and Reporting Authority at http://www.acara.edu.au/

Efforts are being made to coordinate initiatives under DER with the rollout of the NBN. But short term many people – children, parents and carers, students, teachers and school leaders – are poorly prepared for super-fast broadband and global connectivity. Few are positioned to make use of digital technology for informed online engagement and participation, for internet use that may be described as safe, secure, ethical, and productive.

Academics are calling for more Australian research, including studies to evaluate the effectiveness of the various cyber-safety education pilots or programs. This is to build the evidence-based, and inform future programs and developments. There is no question that research will contribute valuable data and yield important insights and understandings. However research and investigation is time-consuming, and can be problematic given the dynamic nature of risks and threats associated with digital technologies and the online world.

Meantime, the matter of safeguarding Australian children and young people online is a real time problem. Their need for cyber-safety education is of today.

RESPONSE IN UK

Roar is also well-placed to comment on the response to current cyber-safety threats in the United Kingdom (UK). Roar Educate operates in the UK market, and has licensed Us Online v2 (cyber-safety interactive learning) to 43 per cent of English government schools.

In 2007 Prime Minister Tony Blair asked Professor Tanya Byron (a consultant clinical psychologist) to conduct an independent review looking at the risks to children from exposure to potentially harmful or inappropriate material on the internet and in video games.

The Byron review was about the needs of children and young people and about preserving their right to take the risks that form an inherent part of their development by enabling them to play video games and surf the net in a safe and informed way.

Safer Children in a Digital World: The Report of the Byron Review (2008)[9], 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'… Regarding the online world, the report proposed that we give children warnings and install filters, but we also must teach them how to keep themselves 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, children will find a way to circumvent them.

Roar believes that by listening to children and young people and putting them at the heart of her Review - and by replacing emotion with evidence – Prof Byron provided some very necessary focus to a highly charged debate about cyber-risk and cyber-safety. Byron's child-centred approach to cyber-safety has prevailed in the UK.

Concurrently in the UK, the *Rose Review: Independent Review of the Primary Curriculum* (2008)[10] – which comes into effect in September 2011 - placed ICT at the heart of the primary curriculum. Rose describes as an 'essential for learning and life' that 'children use and apply their ICT knowledge, skills and understanding confidently and competently in their learning and in everyday contexts; that they become independent and discerning users of technology, recognising opportunities and risks and using strategies to stay safe'.

Following on, Ofsted (the UK regulatory Office for Standards in Education, Children's Services and Skills) earlier this year declared that outstanding schools will have a well-considered, active approach to keeping pupils safe when they are online, and help them to take responsibility for their safety; further, that in an outstanding school responsibility for the safe use of new technologies will be shared by all; that relationships with families will be developed to support e-safety at home; and that the extent and quality of staff training will be improved, and its impact will be monitored systematically[11].

Ofsted school inspections now include evaluation of a school's policies and procedures in relation to cyber-safeguarding, and the safe, ethical and responsible use of digital technologies.

[9] 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/

[10] See *Rose Review: Independent Review of the Primary Curriculum* (2008) by Sir Jim Rose. At http://www.dcsf.gov.uk/primarycurriculumreview/

[11] Ofsted (February 2010). *The Safe Use of New Technologies*. At http://www.ofsted.gov.uk/

Ofsted's position on the use of ICT and particularly its holistic approach to safeguarding across school communities sets the course for cyber-safety education in the UK. It also prompts the shift from 'locked down' to 'managed' systems in UK schools.

In her follow up study, *Do We have Safer Children in a Digital World: A Review of Progress since the 2008 Byron Review* (2010)[12], Prof Byron reports that there is still progress to be made to ensure consistency in the quality of digital safety education in all schools and for all ages, and to develop the knowledge and skills of parents, carers and families.

Byron emphasises the need to make further progress on support for parents, carers and families and their understanding of digital safety issues. She proposes that the Government-guaranteed introduction of online reporting to parents (in secondary schools by 2010 and in primary schools by 2012) is also an opportunity to provide information to parents on child digital safety.

Byron also observes that the inclusion of digital safety in the curriculum is effective only where it is supported by high-quality materials and resources (including acceptable use agreements) that are reviewed and updated regularly, plus the provision of complementary digital safety training for teachers and schools. Byron is adamant that all school staff, not just teachers, share responsibility for digital safety, and hence digital safety training should be provided for all staff. Thus, her *Review of Progress* encourages school leaders to recognise digital safety as a priority for their staff's continuous professional development.

Concluding, Byron recommended that by March 2011 the UK Centre for Child Internet Safety (UKCCIS) publish 'guiding principles for the quality of digital safety materials for schools, children, young people and families'[13].

All this is not to suggest that the UK is on top of cyber-safeguarding for children and young people in the UK. However, Roar submits that three important elements of the UK response merit consideration in Australia:

1 In response to perceived, continuing cyber-risks to children and young people, the UK Government has established a central agency to address child internet safety: the UK Council for Child Internet Safety (UKCCIS)[14]. UKCCIS brings together over 150 stakeholders from across the internet safety spectrum: government agencies, academics and educators, non-government organisations and not-for-profits, plus industry and business sectors.

2 Cyber-safeguarding in the UK is grounded in a positive, proactive view of child internet use. The guiding principle is empowerment through education.

3 To this end, UKCCIS has been tasked with developing and publishing guiding principles and benchmarks for the safe, ethical, responsible use of digital technologies.

[12] Tanya Byron (2010), *Do We have Safer Children in a Digital World: A Review of Progress since the 2008 Byron Review*, Department for Children, Schools and Families. At http://www.dcsf.gov.uk/byronreview/

[13] Tanya Byron (2010), *Do We have Safer Children in a Digital World: A Review of Progress since the 2008 Byron Review*, Department for Children, Schools and Families, page 18.

[14] UK Council for Child Internet Safety, at http://www.dcsf.gov.uk/ukccis/

POSTSCRIPT: REPORT OF CYBER CRIME INQUIRY

Roar's earlier submission[15] to the Australian Government's cyber crime inquiry proposed the development of a national system of certifiable skills standards in Australia. Operating largely as an online program, users would be required to gain certification of a prescribed skill level before being permitted to use the internet in various institutional contexts such as a school or a private organisation.

Roar also argued for broad-based digital literacy training to span cyber safety, e-security, and digital citizenship, and extend even to matters such as intellectual property and online ethics. Both points are reflected in the inquiry's recommendations for a nationally coordinated approach to consumer education tied to clear benchmarks (Rec 31), and the development of IT literacy training (Rec 34)[16].

It is interesting and timely to reflect on the recently published report of the Australian Government's Inquiry into Cyber Crime[17]. The report calls for a more holistic, or whole-of-government approach to tackling cyber crime… 'a commitment to cooperation, strategic thinking and a cyber space perspective to overcome the silos of traditional institutions… current strategy puts an emphasis on education and community awareness but seems to lack the coherence or clear benchmarks for success that might be expected for such an important priority'.

Roar anticipates that similar conclusions as these in relation to cyber crime may be drawn by the present Joint Select Committee in relation to cyber-safety.

[15] Roar Film Pty Ltd (2009). Submission to the House Standing Committee on Communications' Inquiry into Cyber Crime. Submission 64.

[16] House of Representatives Standing Committee on Communications (June 2010). *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*. The Report of the Inquiry into Cyber Crime.

[17] House of Representatives Standing Committee on Communications (June 2010). *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*. The Report of the Inquiry into Cyber Crime. Page ix.

4 opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cyber-safety issues

ROAR OPPORTUNITIES

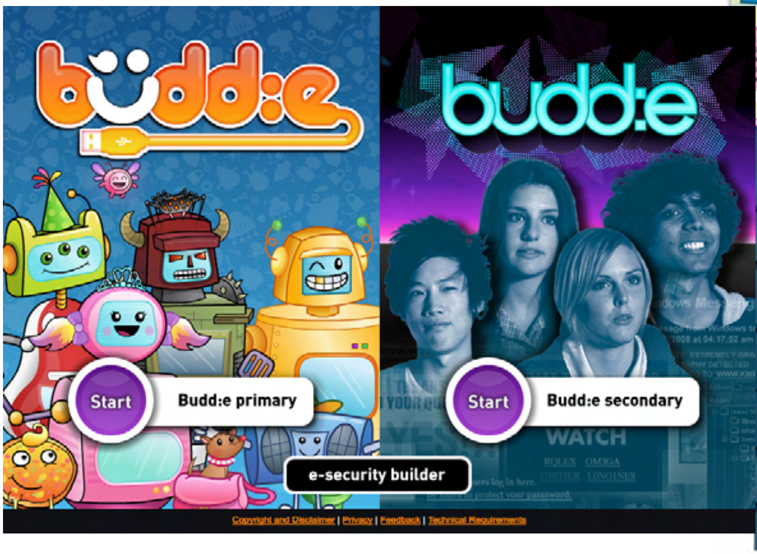
This submission has been informed by Roar's development of interactive content (age-related learning activities and resources) to support teaching and learning about 'citizenship' in the real world and online, including activities and resources to teach children and young people about the safe, ethical, responsible use of digital technologies.

The Roar Educate modules - *Us Online* (K-10) – are licensed to 43 per cent of English government schools. To date *Us Online* is the most successful curriculum content offering on the LGfL content grid, as regards the number of users and the cost per use. *Us Online* was also selected as finalist at the prestigious 2009 BETT (British Educational Training and Technology) Awards.

Us Online is delivered at a cost of 50-75 pence per child per annum. It has proved to be a cost effective strategy for delivering cyber-safety education in the UK. *Us Online* is a dynamic education resource that comes with regular updates: we submit, all benefits of commercial enterprise.

Given the uptake and success of Roar's cyber-safety education in the UK, Roar seeks opportunities to supply comparable product to Australian schools, however the structure of Australia's school education market does not provide any obvious market entry point for an independent operator like Roar.

Concurrently, Roar is pursuing additional ways to cooperate and collaborate with Australian stakeholders. Roar is currently negotiating a UK distribution agreement with DBCDE, to take the *Budde e-security builder* to market in UK. Roar developed these primary and secondary school modules under contract to the Australian Government. *Budde* us at www.staysmartonline.gov.au/budd-e/


budd:e
budd:e
Start
Budd:e primary
Start
Budd:e secondary
e-security builder
Copyright and Disclaimer | Privacy | Feedback | Technical Requirements

Graphic elements from Us Online V2

ROAR RECOMMENDATIONS

With regard to the serious matter of dealing with cyber-safety issues in Australia, Roar recommends the following:

1 Cyber-safety education needs to be mandated, and supported in real ways. In order to genuinely safeguard children and young people online, cyber-safety education must be provided for children and young people, their parents, carers and families, and their teachers and school staff.

2 We submit that it is the proper role of government to establish educational standards – standards for cyber-safeguarding, and the safe, responsible use of digital technologies. Standards are necessary for evidence-based initiatives and programs. Given the health and personal safety implications, agreed standards for cyber-safeguarding need to be a priority of government. We recommend that government in consultation with stakeholders establish educational standards for cyber-safeguarding and the safe, ethical and responsible use of digital technologies.

3 We also recommend that government consider ways to coordinate across the relevant departments and agencies (DBCDE, DEEWR, ACMA, and AMF) so cyber-safety policies and programs are no longer siloed.

4 Beyond the establishment of educational standards and coordination of departments and agencies, government might then step back and allow the market more room to contribute cyber-risk solutions. We argue that Roar (and other education software developers) are well placed to efficiently and cost-effectively serve the cyber-safety education market. After all, government sets road rules and minimum standards for safe, responsible road use, but government doesn't actually teach motorists to drive.

In the UK there are abundant free resources made available to schools, yet Roar has still been able to sell product to more than 40 per cent of government schools. Why? Roar has brought cyber-safety into the domain of citizenship and digital literacy: promoting safe, ethical, responsible use of digital technologies as the social norm online. Roar's content is dynamic and updated regularly. Moreover, at 50-75 pence per child per year, it represents value for money.

5 examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised

A high level of digital literacy would go far towards ensuring that opportunities presented by, and economic benefits of, new technologies are maximised.

The safe, ethical and responsible use of digital technologies is a cornerstone of digital literacy.

Digital literacy education (that integrates learning about e-safety, cyber-security and online citizenship) will greatly assist to consolidate the notion of ‘safe, ethical, responsible use’ as the social norm online.

> *6 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*

In December 2009 former director of the Australian High-Tech Crime Centre Alastair MacGibbon observed, "There is a widening gap between the cyber security problem and our national capacity to deal with it ... It is time to weave internet citizenship education seamlessly into the school system. Children should not just be taught how to use technology, they must be taught how to use it wisely, safely and securely".[18]

Cyber-bullying is but one example of unsafe, unethical and irresponsible use of digital technologies. There are many others. In the digital space, risky behaviour may be sexual (sexting), social (bullying), legal (prohibited content), ethical (copyright), health-related (internet addiction), and so forth.

Roar tackles cyber-bullying with interactive learning (K-10) to explore and establish social norms for online behaviour generally. Roar's strategy brings all aspects into one system: the safe, ethical, responsible use of digital technologies, spanning cyber-safety, e-security, digital literacy, and online citizenship.

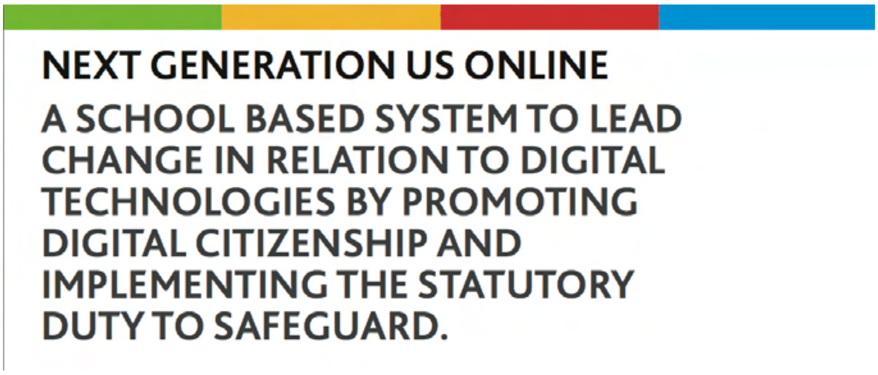
Roar incorporates cyber-bullying within an holistic approach to cyber-safeguarding. Modules include learning activities about safe online identity, netiquette, online gaming, cyber-bullying, social networking, posting content, file-sharing, using the web for research, downloading, privacy, web copyright, secure transacting, viruses and malware, and creating strong passwords.

Positive, protective online behaviours equate to the safe, ethical, responsible use of digital technologies. Learning protective behaviours involves learning about (for example) privacy issues, the permanence of digital content, and the scope one's digital footprint. The positive, protective behaviours that are necessary to protect oneself from cyber-bullying will equally address a range of other anti-social or inappropriate online behaviours.

US ONLINE NEXT GENERATION

Roar's approach to cyber-safeguarding is demonstrated by *Us Online Next Generation*. Roar is currently developing this system for trial in partnership with the London Grid for Learning and the Catholic Network Australia (CNA).

Us Online Next Generation is an online school-based system to promote digital citizenship and assist schools to implement their statutory duty to safeguard. The system caters to four user (stakeholder) groups: school principals and leadership teams, teachers and staff, parents and carers, and students, children and young people.



NEXT GENERATION US ONLINE

A SCHOOL BASED SYSTEM TO LEAD CHANGE IN RELATION TO DIGITAL TECHNOLOGIES BY PROMOTING DIGITAL CITIZENSHIP AND IMPLEMENTING THE STATUTORY DUTY TO SAFEGUARD.

1 For children & young people, *Us Online Next Generation* delivers safeguarding for contemporary learning and life, by enabling and encouraging the safe, ethical and responsible use of digital technologies.

- *Us Online*: standards-based interactive learning (activities for K-10 plus rewards) with assessment modules (mapped to the curriculum) to address topics like safe online identity, netiquette, online gaming, cyber-bullying, social networking, posting content, file-sharing, using the web for research, downloading, privacy, web copyright, secure transacting, viruses and malware, and creating strong passwords.
- Benchmarks for safe, ethical and responsible use of digital technologies, based on best practice and developed in partnership with LGfL & CNA teachers and school leaders
- Assessment regarding the safe, ethical and responsible use of digital technologies against benchmarks
- Automatic reporting of progress and assessment to teachers, and to parents and carers

[18] Alastair McGibbon, from *Cyber security: threats and responses in the information age*, special report no. 26 to Australian Strategic Policy Institute, December 2009.

2 For teachers and school staff, *Us Online Next Generation* delivers teacher professional development (PD) and staff training in the safe, ethical and responsible use of digital technologies; plus resources to support class teaching

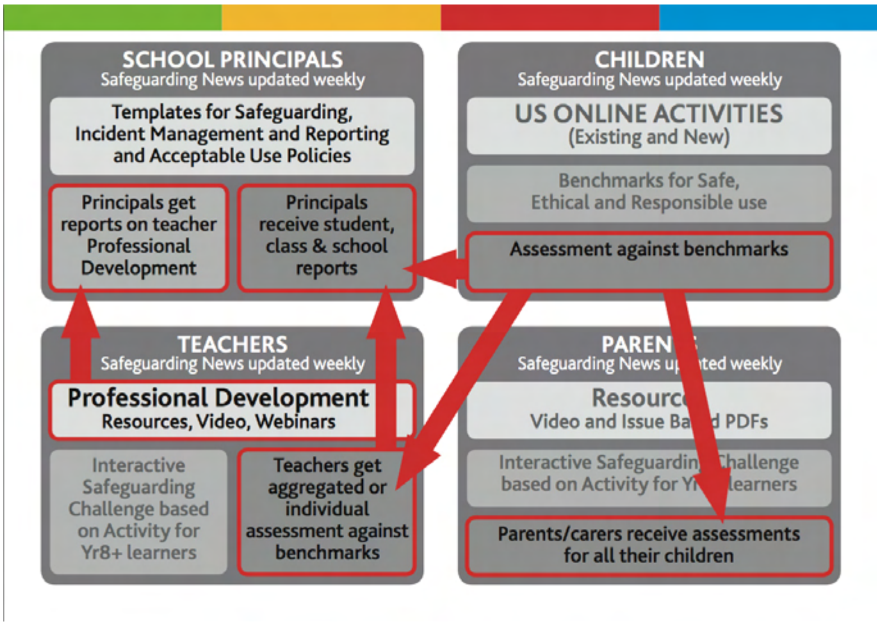
- Issues-based webinars, digital resources and videos for teacher PD and staff training, delivered online
- Us Online interactive 'safeguarding challenge' to simulate issues regarding the safe, ethical and responsible use of digital technologies
- Automatic reporting of teacher PD and / or staff training to SLT
- Portability of individual staff-member PD / training profile across participating school
- Weekly news updates
- Resources to support class teaching and learning about the safe, ethical and responsible use of digital technologies, including interactive learning (K-10)
- Reporting on individual or aggregated pupil progress and assessments against benchmarks

3 For parents & carers, *Us Online Next Generation* provides resources and support for parents, carers and families about the safe, ethical and responsible use of digital technologies

- Issues-based digital resources and videos
- *Us Online* interactive 'safeguarding challenge' to simulate issues regarding the safe, ethical and responsible use of digital technologies
- Reporting on the progress and assessment of their children against benchmarks
- Portability of individual child / young person profiles across participating schools
- Weekly news updates

4 For school principals and school leadership teams, *Us Online Next Generation* provides resources and support for principals to carry out their statutory duty to safeguard in the digital space … safeguarding for pupils, staff and data.

- A system to manage digital safety education and training across the entire school population (staff and students)
- Templates for safeguarding (children and young people, teachers and staff, and data), incident management and reporting, and acceptable use policies
- Benchmarks for safe, ethical and responsible use of digital technologies, based on best practice and developed in partnership with LGfL teachers and school leaders
- Reporting on individual or aggregated student progress and assessments against benchmarks
- Reporting on individual or aggregated staff progress in relation to teacher PD and / or staff training
- Weekly news updates


SCHOOL PRINCIPALS
Safeguarding News updated weekly
Templates for Safeguarding, Incident Management and Reporting and Acceptable Use Policies
Principals get reports on teacher Professional Development
Principals receive student, class & school reports
CHILDREN
Safeguarding News updated weekly
US ONLINE ACTIVITIES
(Existing and New)
Benchmarks for Safe, Ethical and Responsible use
Assessment against benchmarks
TEACHERS
Safeguarding News updated weekly
Professional Development
Resources, Video, Webinars
Interactive Safeguarding Challenge based on Activity for Yr8+ learners
Teachers get aggregated or individual assessment against benchmarks
PAREN
Safeguarding News up ted weekly
Resourc
Video and Issue Ba d PDFs
Interactive Safeguardin hallenge based on Activity for Y learners
Parents/carers receive assessments for all their children

BENEFITS: US ONLINE NEXT GENERATION

- *Us Online Next Generation* is an intelligent system, designed to:
- Integrate all aspects of digital safeguarding, and the ethical and responsible use of digital technologies
- Share the responsibility for safeguarding appropriately, and empower all parties
- Promote best practice in relation to the safe, ethical and responsible use of digital technologies
- Address real-time problems of the online world
- Support the Australian Government cyber-safety and security agenda
- Support the Digital Education Revolution
- Align to MCEECDYA's Statements of Learning for ICT in relation to safe, responsible, ethical use of digital technologies
- Provide data and reporting to inform the evidence base
- Facilitate the transition from locked down to managed systems
- Equip school leadership teams
- Support and resource teachers, and relieve them of the need to consult multiple resources
- Support the school / home / community continuum, and promote parental engagement
- Reduce the digital divide within families
- Define a new model for the delivery of online content
- Embrace Web 2.0 and promotes its creative and constructive use
- Provide a safe framework to lead change in relation to the use of digital technologies across Australian schools
- Consolidate a system for cyber-safeguarding for school leadership teams, staff, students and parents

7 analysing information on achieving and continuing world's best practice safeguards

Us Online Next Generation is an assessment, reporting, and information gathering system.

Us Online Next Generation assesses cyber-safeguarding issues across all age groups, and is constantly updated.

Us Online Next Generation will contribute valuable data about the cyber-safety of Australian children and young people, and cyber-safeguarding practice in Australian schools.

8 the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues

(no comment)