ABN 46 090 549 947
T 1300 737 060
F 1300 737 069
PO Box 396 Fortitude Valley
Qld 4006 Australia
info@netboxblue.com
netboxblue.com

Submission to
Joint Select Committee on Cyber-Safety

Author – John Fison, Chairman, Netbox Blue P/L

23rd June 2010

Netbox Blue commends the Government in setting up this Committee and its pursuit of solutions to improve Cyber-Safety for children in Australia.

Netbox Blue applauds the initiatives that have been introduced including the recent Cyber Security Awareness Week, for which Netbox Blue was one of the partners.

Netbox Blue wishes to contribute to the following terms of reference of the Committee:

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);
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 (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking);
    - identity theft; and
    - breaches of privacy;
iii. Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) their effectiveness and costs to stakeholders, including business;
iv. opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cyber-safety issues;
v. examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised;
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;

vii. analysing information on achieving and continuing world's best practice safeguards;
viii. the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues; and

About Netbox Blue

Netbox Blue is a privately owned internet management company, based in Brisbane, with offices in Brisbane, Sydney, Melbourne and international offices in Taipei and London. Netbox Blue provides schools, businesses and government organisations with the tools to protect their networks from internal and external threats, control data leakage and ensure staff and students use the internet safely and productively. The company offers a broad portfolio of products and services including Social Media Management Systems, Unified Threat Management appliances, email filtering appliances and web filtering appliances. Established in 1999, Netbox Blue now has a presence in 19 countries and has partnerships and distribution agreements with some of the world's largest IT companies.

Netbox Blue has operated in the secondary education market in Australia over the last 5 years. We supply total internet, web filtering and email management solutions to many of the biggest schools across Australia.

Netbox Blue has formed partnerships with various independent schools educational bodies, including the following:

- Christian Schools Australia
- Associated Christian Schools Australia
- Association of Independent Schools WA
- Association of Independent Schools QLD

Netbox Blue's technology has been adopted in the Education sector due to the following reasons:

- Ease of use
- All-in-one solution
- Reliability and effectiveness of its core functionality (security, virus and spam filtering), etc.
- Its innovative technology to deliver a safe environment for students

Netbox Blue has devoted the last three years to developing patent-pending and unique technology to address the issues highlighted in the terms of reference – especially around cyber bullying, exposure to illegal and inappropriate content, inappropriate social and health behaviours in an online environment and breaches of privacy.

Specifically Netbox Blue has developed innovative, patent-pending and award winning software to prevent inappropriate conversations or communications from occurring on common social media applications such as Facebook and Twitter. This technology can be deployed at schools, on laptops provided by the schools to be used outside of the

school's network (this has previously been outside of their control) and, soon, at home on the families' PCs.

This technology is now being used by schools across Australia and Netbox Blue is preparing for the launch of its standalone product for parents to use at home, CyberSafehouse.

Netbox Blue has won several awards for its innovation in this area and has Education customers from Independent, Catholic and State schools.

Netbox Blue is an active member of the Internet Industry Association (and has recently been a member of the e-security subgroup).

Netbox Blue subscribes to rigorous testing of products that can be used by schools and families and is a supporter of initiatives such as the Family Friendly Filter. Netbox Blue's technology has successfully been awarded this accreditation.

Netbox Blue has gained significant experience from providing solutions to schools across the country, working with education bodies, talking with Principals, Deputy Principals, Pastoral care teachers, Heads of Years, Business Managers, IT Managers and parents. Most importantly Netbox Blue has a very and broad understanding of how students exploit vulnerabilities in current technology solutions and has put forward summary recommendations on how this may be addressed.

Netbox Blue's seven findings

1. School administrators and associated groups and bodies have no access to independent advice or a "blueprint" on how to tackle the issues described in the Terms of Reference.
2. As a result, these schools spend an inordinate amount of their limited time and resources in investigating solutions.
3. Thus schools often deploy inappropriate solutions and often do not receive value for money.
4. The threat of cyber safety, privacy, access to inappropriate material, cyber bullying and other undesirable web-based activities has spread beyond simple email and web browsing.
5. The emerging threats come from Facebook, Twitter, YouTube and other social networking sites.
6. The threat landscape has moved beyond schools' networks to any WIFI or home network that provides laptops to students. Many laptops are unprotected outside of the school network.
7. Many advisors to the education sector provide well-intentioned but limited advice that on the full array of threats or how to deal with them.

Recommendations

Netbox Blue can provide advice and research on its findings into the provision of tools to parents for home use. It has conducted user analysis studies, workshops and independent research into parental needs and awareness of solutions.

When it comes to student safety on the internet there is no single solution. A number of "pillars" need to exist before there is any chance of success in combating the multitude of growing threats.

We recommend promoting and enforcing "acceptable use policies":

1. The creation of an acceptable policy framework and its communication to all stakeholders - students, teachers, parents and carers.
2. Education for all stakeholders on minimising known risks, or dealing with them if presented with a situation that places them at risk – focusing on working with students, teachers, parents and carers.
3. Technology enforcement – in and outside the school network on all school owned equipment.
4. Regular reviews of attempts to breach such policy frameworks to improve education and to manage individual behavioural issues.

Netbox Blue witnesses the providers of these individual services and advisors / consultants regularly stating publicly that their unique area of expertise is the only possible way of solving the issues and that the other necessary pillars are irrelevant. In many cases these views come from authoritative sources, such as leading academics who are looking into the issues of cyber bullying. Netbox Blue applauds leading academic institutions such as at Edith Cowan University in WA which is actively looking for complementary providers of solutions to help tackle the issues they research.

The following activities could be undertaken to promote the availability of solutions and to encourage their adoption:

1. Establish a central body to provide advice and online collateral, papers, policies and best practice examples to schools.
2. Establish a framework (as recommended in Netbox Blue's four pillars point) and establish a certification for providers within each "pillar", such as the Family Friendly Filter scheme.
3. Research and establish a clear set of standards for a school to have achieved to fulfil their duty of care and to provide reassurance to all stakeholders that the school is "certified".
4. Establish a national certification standard for schools (K-12) across all sectors (Independent, Catholic and Public) in providing a Cyber Safe environment for students.
5. Promote the program to all schools and encourage them via grants or other appropriate incentives to benefit from adherence to the Standards.

6. Then promote the program to all other stakeholders to provide reassurance that a National Standard is in place and that their school has (ideally) met the criteria.
7. Establish an ongoing review of the Standards and an annual re-accreditation to ensure ongoing compliance and communications to each new year of student intakes. This could be done without the need for additional expense by requiring all 4 areas to be "signed off" by accredited suppliers within their area of expertise.

The benefits of this path will be:

- Schools will embrace the program as it offers them reassurance of a centrally provided and thoroughly researched set of Standards that offer them a Certification that they will be proud of.
- Schools will be able to spend less time pursuing individual research into how to solve the same issues that face every school in the country.
- Schools can be advised as to where the boundaries of their "liabilities" are with relation to their duty of care (specifically relating to laptop provision and what their responsibilities are in managing these outside of the school's network).
- Less money will be wasted on a "trial and error" approach of individual States and school bodies / schools tackling the issue in different ways.
- Standards can be set to ensure that the rush of advisors, consultants and technology suppliers meet a set of pre-determined standards and deliver advice or solutions within the framework that may be agreed.
- Specifically technology suppliers should be required to demonstrate reference-able capabilities in tackling Cyber Safety for children (see further recommendations below).
- Federal Government can provide common frameworks and support to State based and Independent and Catholic school bodies. This can include legal frameworks and communications tools to ensure adherence to the standards.

From the supply of technology solutions perspective Netbox Blue would recommend that the Standards require suppliers to be able to demonstrate compliance with the following capabilities that are vital if schools are to fully discharge their duty of care to students:

- Time of day restrictions and quotas (data and time) for all school owned equipment (including laptops that are used outside of the school's network). This addresses the issues of technology addiction, amongst other necessary benefits.
- Advanced web filtering capabilities that meets stringent criteria as demonstrated by the Family Friendly accreditation, perhaps adopted specifically for schools.
- Use of a test framework to validate compliance with the standards that are agreed and specifically to ensure that any accredited solutions are capable of withstanding student attempts to obviate their controls. This is a vital component to ensure confidence in the accredited suppliers and Standards. (Netbox Blue has vast experience in understanding how students will push the boundaries of filtering and cyber safety control software and can provide advice based on its own experience and test frameworks that it has developed).

- The ability to specifically manage the points mentioned in point (a) ii. In the Terms of Reference for laptops that are provided to students for use inside and outside the school's network. This should extend to content filtering and application control over social media applications and prevent these from being used as a cyber-bullying tool or indeed for the other issues highlighted in this Term of Reference.
- Specific guidelines to be in place for Facebook to help schools and students deal with privacy, cyber bullying and cyber-stalking threats.
- Advanced reporting and alerting abilities to identify any attempted policy violations to enable early behavioural management to be instigated.

Netbox Blue would further advocate that once the Standards are established that all other associated stakeholders be involved in an education program to provide awareness and collateral to them to pass on as necessary. This would include the State and Federal Police departments (who have task forces focused on Cyber Safety), Parent organizations (e.g. P&C bodies), Educational bodies across Australia and ISPs.

Furthermore, Netbox Blue would suggest that a central legal counsel be established to provide advice, to schools. This advice should cover standard communications and also how to deal with violations or attempted violations of the Standards. This again will save schools enormous amounts of money and time and ensure they gain access to the best advice that is consistent from school to school.

The concept of an online ombudsman is a matter on which Netbox Blue has no firm views. On the one hand it can be helpful to establish such an office similar to (say) the Banking, Insurance or Telecommunications Ombudsman.

On the other, the fact that legal jurisdiction is uncertain especially for the most popular networking sites, could lead to merely another layer of mediation without any real power.

It is something that would require legal coordination across several international borders. It would be useful to clarify where the gap exists and how an online ombudsman can fulfil such roles as against other mediation options available.

Netbox Blue would be happy to elaborate on any of the points raised in this submission and indeed to provide further details pertaining to any aspect of interest to the Committee to help address the issue of Cyber-Safety for children in Australia.

Netbox Blue once again commends the Committee in investigating this rapidly growing set of issues and hopes that it can help work with the Committee in formulating a set of recommendations for Parliament.

For further information please contact John Fison, Chairman, Netbox Blue.
1300 737 060