"Implementing an Integrated National Cybersafety Programme for the Compulsory School Sector"

Douglas Harré
Senior ICT Consultant
Ministry of Education,
Wellington, New Zealand
douglas.harre@minedu.govt.nz

Keeping students safe in an increasingly pervasive digital environment has been a challenge for many jurisdictions around the world. This task is usually undertaken by one or more relevant government departments within a country. Since 1999 the Ministry of Education in New Zealand has funded the provision of a range of cybersafety initiatives that have resulted in a comprehensive, integrated approach to this issue.

This paper shows how the Ministry of Education has achieved this through the use of an "agent of choice" – The Internet Safety Group, and the co-ordinated education-focussed approach the Ministry has adopted in implementing this range of programmes. It also examines 2 associated initiatives this partnership has had a role in.

Keywords: Internet safety, forensic audits, school governance, managed internet services, Digital Strategy

Introduction:

Like many countries that wish to best take advantage of the new economic and social opportunities offered by a "digital world" New Zealand has implemented a range of programmes over the past decade years to enable developments in the ICT and associated sectors to flourish. As with all such programmes there have been variations in the success of such initiatives due to a variety of factors, be they political, financial or organisational. While the Lord of the Rings trilogy was a global success cinematically and made the American backers very happy financially, the development of the software to render the scenes and the broadband connections to transmit them to the editing studios was a reminder of the range of technologies now required to make films (and money) in the 21st century.

Background to New Zealand’s ICT Strategy

During the 1980s and 1990s a number of generic documents were produced that were aimed at using "computers in schools". However the rapid development of information and communication technologies (ICTs) within society was only officially recognised for the first time in 1993 by inclusion within the New Zealand Curriculum Framework. All seven compulsory curriculum statements of the broad aim that; “Students will become competent in using new information and communication technologies...” (Ministry of Education, 1993, p.18). The Technology curriculum (MOE, 1995), which could have been expected to contain a strong ICT component, has a focus on a variety of technology strands such as biotechnology and food technology. It was not until 1999 the Ministry of Education released “Interactive Education”, the first dedicated ICT strategy document for the compulsory school sector. In 2002 this was replaced with "Digital Horizons, Learning through ICT". The strategy prioritises working in partnership with families, communities and businesses to share knowledge of ICT.
and provide opportunities for learning through ICT. Work is currently underway on the third iteration of this strategy for release in 2006.

Other countries at the same time were producing documents of a similar flavour, most of which contained an internet safety component. In New Zealand a number of organisations were similarly interested in this work and with the release of “Interactive Education” initial approaches were made by a number of them to the Ministry of Education for some form of seed funding.

While this may appear to some as an unusual approach it was in keeping with a number of other similar initiatives at that time. One result of the wide-ranging education reforms (known as Tomorrows Schools) that took place in New Zealand in 1989 was that much curriculum and resource delivery began to be contracted out to specialist organisations. These were seen as more able to quickly and efficiently address the needs of a number of differing organisations. The Ministry recognised early on the value of the recently-formed Internet Safety Group and the influential cross-section of organisations it had already marshalled. These included the New Zealand Police, various Internet Service Providers, Auckland Rape Crisis, SAFE Network (a sexual offenders’ treatment programme), and secondary school senior management. This grew rapidly to include a variety of agencies and community groups concerned about children’s safety: Child, Youth and Family Services, primary and intermediate schools, parents, School Boards of Trustees, students, the Peace Foundation, ECPAT (End Child Prostitution and Trafficking), the Department for Courts, and the Department of Internal Affairs and their associated Censorship Compliance Unit. Launched in March 2000 the original ‘New Zealand Internet Safety Kit’ was produced by the group for use in schools, with sponsorship from the Ministry of Education, Child, Youth and Family Services, and New Zealand Police, and also endorsed by the Department of Internal Affairs. The kit was sent out under the auspices of the Ministry of Education to every school in the country, both public and private.

In addition to the work carried out by this organisation the Ministry also provides providing infrastructure required to establish safe and secure internet access through the Managed Internet Services (MIS) Project (see Case Study 1 below).

Ongoing Funding of the Internet Safety Group

The government through the Ministry of Education has since been the prime funder of the Internet Safety Group (ISG) since 2001. From a funding level of around $300,000 per year the allocation for FY2005 amounts to almost NZ$1million. This funding covers the sponsorship of the ISG’s director, the NetSafe Kit, training modules, the Netsafe website, conference sponsorship and a research component. It also contributes to other cybersafety work that the ISG does in the wider community. This is in keeping with the ISG’s philosophy that its role is to inform and educate individuals, groups and organisations, and empower them to put into effect cybersafe programmes and practices.

This core funding is seen as providing security and staffing to actively manage and leverage relationships and funding from the wider education and business sectors. This has been a very successful strategy with additional sponsorship (financial and in kind) from a range of companies including software companies, banks and educational trusts. Also of benefit are the substantial cost benefits of consistent and collaborative approaches to cyber safety across a variety of government agencies, both in terms of developing training material and the generation of policy. In an environment where government expenditure is closely monitored there are also savings able to be made due to lack of duplication of services and expertise.
Much of this work is now connected at a higher political level to the recent release of “The Digital Strategy” an overarching strategy and integrated framework for government initiatives to encourage the uptake and effective use of ICT in New Zealand. The Digital Strategy "describes the necessary conditions for New Zealand to become a world leader at using information and technology, proposes actions for realising the benefits of ICT in communities, in business and in government, identifies the opportunities and challenges facing New Zealand and outlines the Government's role in addressing them” It is a core element of the Government’s Growth and Innovation Framework was set up to provide a cross-sector and regional platform for growth in a wide range of areas. In this document a range of cybersafety issues are discussed ranging from viruses and the challenges of online banking to accidental exposure to online pornography.

At the heart of the Digital Strategy is the integration of the three C's - connection, content and confidence:

- Connection is about being able to gain access to affordable and viable ICT infrastructure such as broadband, computers, mobile phones and other devices
- Content is about gaining seamless, easy access to the information all New Zealanders find important for their lives, businesses, and cultural identity
- Confidence is about creating the environment where all New Zealanders can gain the digital skills to find and use the information they need; and to ensure that telecommunications and the Internet in New Zealand are reliable and secure.

In terms of the Digital Strategy cybersafety will be addressed in the Confidence section, and it will be interesting to see how the work carried out primarily thus far in the school sector is translated to the wider community.

**Case-study 1: Managed Internet Services (MIS) Project**

Through the MIS Project, the Ministry of Education committed NZ$9.8 million to providing a suite of managed internet services free to all state and state-integrated schools. (the latter being non-private schools that usually have a religious component) This funded:

- A hardware firewall
- A number of content filtering products to prevent the access of inappropriate websites
- Email filtering to prevent the sending or receiving of offensive material and oversize attachments
- Management of spam and junk emails such as chain letters, jokes, image files and screen savers
- Usage monitoring and reporting.

In New Zealand’s self-managing school environment none of these products can be mandated at a national level, and schools are generally keen to reduce what they see as centralised decision-making by the Ministry of Education. One of the by-products of a series of major education reforms of the late 1980s is that schools have been free to choose their own technology platforms. This has resulted in a multiplicity of platforms and as an increasing number of schools begin to ask for assistance in this area the government has had to provide a number of solutions to cater for a wide variety of installations. As the
expectations of users has grown, and the financial implications for schools have skyrocketed also, there has been a realisation that many products and services that are IT-related (e.g. national licensing agreements for the provision of software from companies such as Microsoft and Apple, and the hardware provided through TELA, the national laptop rollout project) can be provided much more cost-effectively through some form of bulk-purchasing.

Small primary schools in particular have been keen to take up this offer – around 25% of New Zealand’s 2650 schools have a roll of less than 77 students, and with allied programmes providing incentives to move from dial-up to faster DSL connections many were concerned about cybersafety and security implications of such a move.

Schools now have a choice of four products that they may implement in their school. Two are monitoring and filtering packages that offer a fully managed, remotely hosted solution. Designated staff in schools can block or unblock sites at will through a web interface, and may choose, if they wish, to not block sites at all but merely monitor them. For many schools and their communities this provides some measure of comfort. Two more choices available to schools are in-house, server-based products that require more specialist support.

All products also filter out spam, which is a major irritant in all school inboxes. All products are available to schools at no cost, and there is no mandate from central government to use one. The rationale is – “we have tested these products, bought them at a discounted price and therefore you can use them with a degree of confidence, if you wish”.

By August 2005 around 60% of New Zealand schools were using one of the four products. This project has been generally successful, although the potential pitfalls of this approach were illustrated recently when a senior student at a large Auckland high school found his favourite anarchist website had been blocked by the newly installed filtering system. While this was resolved relatively easily, the case went around the world very quickly (spurred on by numerous bloggers) and generated a large number of emails and media requests very rapidly. Once again the ability to bring in the ISG as an independent entity was of great assistance in showing that this was not part of the Ministry of Education’s desire to close down political debate in schools.

The technical limitations of these products and their links to various religious and/or right wing organisations have been well documented by numerous writers (e.g.Willard 2003). The well-known local example in New Zealand is of a senior economics class that had to visit the websites of local real estate agents. When visiting [www.ljhooker.com](http://www.ljhooker.com) they were blocked by the filtering device. However many parents report anecdotally that they are happy to have one such site blocked temporarily if it means that a multitude of less pleasant sites are kept out.

Various civil liberties and librarian organisations in the USA in particular, have mounted legal challenges and public campaigns against the use of such filtering and blocking devices in schools, libraries and other public institutions. The most well known of these has been United States v. American Library Association case 02-361, in June 2003. The US Supreme Court ruled in a majority decision that the Children’s Internet Protection Act (CIPA) does not violate First Amendment speech protections through it’s requirement that libraries or schools that receive federal assistance to install software that blocks obscene or pornographic images. While it may be quite right to say that “a teacher with responsibility for ICT may well relish a debate about the need to protect children from unsafe internet
exposure versus the importance of freedom of information, the technical issues involved with filters can be massive” (Hope, 2003) it is hoped that the MIS project will provide ease of use through a remotely managed solution, as under the Ministry of Education’s National Administration Guideline 5, schools are required to maintain a safe physical and emotional learning environment. The provision of the tools outlined above is to assist schools who wish to make that particular choice.

In 2001 the Education Review Office reported that 82% of schools were taking steps to address the inappropriate use of the internet. Since then anecdotal evidence and increased awareness suggests almost all schools have policies and practices related to cybersafety. In early 2005 ERO reports on e-learning stated that only 15% of primary schools and 18% of secondary schools saw Internet safety as being a challenge, compared with the larger perceived issues of funding new equipment (79%) or maintaining existing equipment (70%). Whether this is a slightly head-in-the-sand approach or an accurate reflection of the wider and for them more pressing problems facing schools wishing to implement ICT is a matter for further research.

**Case Study 2: Forensic Audits**

In response to a number of high profile stories during 2003/4 concerning inappropriate material found on school computers the Ministry of Education funded a forensic audit of school computers. A random selection process generated approximately 100 schools that covered a range of rural/urban, primary/secondary and socio-economic indicators. These schools were then invited to be part of the audit process and 26 agreed to be audited.

Schools taking part were guaranteed anonymity, although all schools were informed that any material that was found to be contrary to the relevant legislation (the Films, Videos, and Publications Classification Act 1993) may result in proceedings occurring as it is the professional duty of the forensic specialist to inform the police or the Department of Internal Affairs Censorship Compliance Unit (just as it is the duty of a school to inform one of those two authorities if the school discovers such material has been deliberately accessed).

Material that was deemed to be inappropriate from an employment perspective would be referred to the employing authority, in the New Zealand case this being the Board of Trustees of the relevant school. Due to the myriad of issues that could arise from this situation the audits were carried out in done in close participation with the School Trustees Association, national teacher unions and principals associations. Even though the schools volunteered many exhibited some early and understandable concern about how the results may be interpreted and used against their members.

Teacher unions in particular were concerned about the results potentially impacting on their members and the feedback from some schools was that a number of teachers were unhappy with being told that “their” laptop was to be audited. This resulted in one teacher leaking the audit process to a journalist on a national newspaper and thereby putting at some risk the Ministry’s undertaking of confidentiality.

The audit process itself was carried out by a highly qualified and experienced electronic forensic organisation which provides services to a range of bodies such as the New Zealand Police Force, Military and Employment Court. Given that legal
Proceedings may have been a possibility all work carried out was of a standard that would be subsequently admissible in a court of law.

Only images were audited, with a total of 21,988,179 being copied from the computers’ hard disks. Upon analysis the total number of inappropriate pictures was 4,135. This is 0.019 % of the reviewed pictures. Of the images, their categorisation within the five categories as a percentage of the total inappropriate images was:

- “Calendar style” pictures 35 %
- “Jokes” 4 %
- “Naked Images” 23 %
- “Hardcore Pornography” 36 %
- “Objectionable Images” 2 %

Inappropriate images were found in all levels and types of school, state, integrated, private, co-educational and single sex. Interestingly boys and girls single-sex schools had the same percentage (11%) of inappropriate images.

While the sample size was relatively small (in terms of numbers of schools) it appears that this may indicate that the public perception that school computer networks are seething with the downloaded pornography of teenagers (or teachers) may not be entirely true. Other internet activity potentially both work and non-work related was noted without any estimate of the amount of activity. These activities included:

- On-line shopping
- Travel
- Hobbies/Interests (i.e. car parts/fixing)
- Gambling
- Medical
- Children interests (cartoons, etc)

The audit report did not consistently identify the origins of the material, whether it was sourced accidentally or deliberately or whether it was downloaded by students or school staff. Many of the images identified by the auditor were not in a form or place that was easily accessible.

The management of schools taking part in the audit were then invited to a national series of meetings organised by the Ministry of Education. They were provided with an overview of the forensic methodology and the results at a national level. Each school was provided with their individual findings – as part of the Ministry’s agreement with the schools the individual school results were not to be made available unless any school wished to do so (again as employment issues are a matter between the school and their Board of Trustees). The auditor commented that the number of inappropriate images discovered on the school computers was significantly lower than similar forensic audit tasks he has conducted outside the school sector.

As a by-product of this success of process the Ministry of Education offered to pay half of the costs of any school who wished to have a similar audit carried out in their school. As a result a relatively small number have chosen to do this – sometimes on a suite of computers and in other cases a single computer being used by one person where some concerns have been raised.
The non-compulsory sector

While this paper is concerned with the compulsory sector there have been contrasting developments in the early childhood and tertiary sectors. In response to calls from those working in the early childhood sector “Foundations for Discovery, an Early Childhood Education ICT Framework” was released in April 2005. This resource sets out an overall vision and guiding principles for the use of and investment in ICT in an early childhood education setting. It does clearly state in the section Strategic Focus Area 5: Building Infrastructure, Systems and Standards ...(that) “the government will ...provide guidelines to inform ECE services' decisions in the areas of: health and safety, including Internet Cybersafety”. This can be contrasted with the Tertiary e-learning framework document released the previous year which while being justifiably concerned with digital rights management, communities of practice and flexible learning pathways has nothing to say about cybersafety in that sectors institutions. These contrasting approaches may just reflect the technological differences in the sectors and target demographics of the students, but it may also illustrate a certain complacency in the approach of those involved in higher education.

Conclusion:

From the Ministry of Education’s perspective the approach of working with an “agent of choice” has resulted in a series of initiatives that have had far-reaching impact in New Zealand and internationally. The imagination, credibility and buy-in that has occurred is possibly greater than if it had occurred as a standard government initiative, partly due to the fact that the opportunity has existed for ISG to broaden their scope to include sectors other than education, but all the time keeping education as their focus. The business sector in particular is realising that education for their users is also a major issue. Ongoing media coverage around inappropriate use of computers in work time ensures that this issue is very much in the public eye.

In terms of schools awareness it is undeniable that awareness of the complexity of cybersafety issues has grown markedly in the last few years. The freefall in computer hardware prices, the national growth of broadband connections and the increasing pervasiveness of the technologies has placed extra pressure on education and other government agencies. When it is factored in that considerable sums of money have been invested in providing New Zealand schools with the use of new communication technologies, it is not unreasonable to view the delivery of cybersafety training (through initiatives such as the modules) as a high priority.

This approach fits in well with the self-managing, devolved decision-making nature of the New Zealand education system where principals, schools and their Board of Trustees value the opportunity to make decisions locally based on local knowledge and community desires. From a governmental viewpoint the opportunity to collaborate in a cross-departmental framework with dedicated and imaginative people who are committed to their work has been of great value also.
Bibliography


