

Computer Security for New Zealand Schools

Written by:
Warren M Anderson (MIS, ITCP)
computersecuritynz at gmail.com

Special thanks to:

Andrew Hooker (LLB) - *lawmannz at gmail.com*
Stephen (Skip) Parker (MCSE) - *skip at ignition.net.nz*
Steve Riley - *Stvrly at gmail.com*
Dave Simpson – *dave at funkypancake.com*

for contributing to the development of this document.

Version 1.6 as of March 8, 2010

Please send any suggestions for changes/additions to:
computersecuritynz at gmail.com

Distributed under the
Creative Commons Attribution-NonCommercial-ShareAlike (New Zealand) License 3.0.

Executive Summary

The Internet is now an integral part of the New Zealand education system. It is used by pupils to research information, communicate with other students and increasingly for submitting home work assignments. This brings enormous opportunities for pupils as they learn to essential online life skills which prepare them for life after school.

Teachers too benefit from being able to make use of online resources both in lessons and for their own research and it's not uncommon for teachers to have remote access to their school network and emails from home using a laptop or home computer.

However, there is growing concern that our teachers are being left vulnerable to online threats which have the potential to threaten their professional reputation and even their very livelihood. One recent case saw a well respected New Zealand head teacher falsely accused of accessing inappropriate material on his computer. Despite his innocence, he lost his job, his home and has since moved abroad. There was also reputational damage to the school.

This paper is written in response to this and many similar cases. It seeks to bring wider attention to these issues and offers some guidance on steps which can be taken to minimise the risks to schools and teachers.

Guidance in the document is addressed to three groups:

- **Schools** (as employers) have a responsibility to protect their employees. They must work with their Network Administrators to ensure their networks are set up correctly and that teachers (and other educators such as principals) have the right support. Most importantly, schools are provided with guidance on how incidents should be investigated to protect the integrity of the school and give the teacher a fair hearing.
- **Teachers** (as employees) have a responsibility to protect themselves. A few simple changes to the way a teacher uses their computer can minimise the risks of being falsely accused of accessing inappropriate material.
- **School network administrators** have a responsibility to protect their users. A number of more technical recommendations are addressed to this group.

Building on existing Ministry of Education guidance, the recommendations in this document seek to strike a balance between the rights of teachers, the usability of computers systems and, of course, the protection of our children.

The ultimate goal is to provide a safe and secure IS environment in schools which allow teachers and children to make the best use of the benefits that this technology can provide. This paper is our contribution to this aim.



Warren M Anderson

Contents

Executive Summary.....	3
1. The Schools Responsibility.....	6
1.1. <i>General Recommendations</i>	6
1.2. <i>Passwords</i>	7
1.3. <i>Content Filters</i>	7
1.4. <i>The Forensic Analysis</i>	8
2. The Teacher's Responsibility	10
2.1. <i>Desktop</i>	10
2.2. <i>Passwords</i>	10
2.3. <i>Avoid Adware and Spyware</i>	11
2.4. <i>Be Aware of Phishing</i>	11
2.5. <i>Electronic Communications</i>	12
2.6. <i>Usage agreements</i>	13
2.7. <i>Inappropriate Content</i>	14
2.8. <i>Suspicion is conviction</i>	16
2.9. <i>The Forensic Analysis</i>	17
3. The School Network	18
3.1. <i>Operating System</i>	18
3.2. <i>Desktop</i>	18
3.3. <i>Security Tweaks</i>	19
3.4. <i>Passwords</i>	19
3.5. <i>Email Clients</i>	20
3.6. <i>Content Filters</i>	20
3.7. <i>Malware</i>	20
3.8. <i>Manage the Browser Cache</i>	21
4. Conclusion.....	22
5. Glossary	23
6. References	24
Appendix A – MoE Initiatives	28
Appendix B – News Articles.....	29
Creative Commons License.....	30
Contributor BIOs.....	31
Acknowledgements	32

1. The Schools Responsibility

In this section some suggestions are made on how schools can act to provide tools and protection to their staff. It also explains how a school should respond if it is required to investigate a member of staff to ensure the evidence is collected and analysed correctly for the sake of both the school and the individual under suspicion.

The Ministry of Education has put considerable effort into providing quality ICT programmes for New Zealand schools¹ and working with schools to provide a safe physical and emotional environment for their students. The schools then pick up these recommendations and implement them to the best of their abilities. The problem this presents is that each school has its own constraints and priorities which are likely to impact on how well the ICT programmes are implemented.

In his 2002 paper titled “*Internet Safety: Issues for New Zealand Primary Schools*” Dr John Hope, the Director of Primary Teacher Education at the University of Auckland, expressed unease about ICT funding when he wrote:

“Provision of an adequate ICT budget is a major concern for New Zealand primary schools who, until recently, were expected to fund all capital and professional ICT expenditure from within an operating budget unchanged from the period before ICT arrived in schools.

...In financially strained circumstances such as this, extra costs for internet safety become an issue. Even a cost as small as \$40 per month for a filter such as Watchdog is subject to intense lobbying when a classroom teacher has a computer but no printer.

...Faced with a choice between network extension and implementation of net security, it is likely that some schools will opt for extension of the network first.”
(Hope, 2002)

Making IS decisions based on budgetary constraints or insufficient knowledge presents a risk to the school’s employees, as it encourages schools to adopt poor quality solutions in preference to more robust ones. When the issue at stake is the security of the school’s network and the protection of their employees, it was inevitable that sooner-or-later, the system was going to break down and someone was going to get hurt.

1.1. General Recommendations

- It is important that the advice and directives of the Ministry of Education, the Department of Internal Affairs and Netsafe, regarding networks and the Internet, be understood and adhered to.
- If you have a Network and/or Internet Usage Agreement which asks your teachers to confirm that they have sufficient knowledge to safely supervise the school’s network, Internet access, computers, webcams and other ICT equipment (Netsafe 2006a) ensure

¹ See APPENDIX A

that they understand what they are committing themselves to and if necessary, provide additional training.

- Work with your school's IS team to agree on the recommendations that should be put in place. That way the Board-of-Trustees and principal will have some understanding of the risks they have taken on and the protections they have put in place, before they are faced with a computer-related incident.

1.2. Passwords

A username and password are the typical method for securing access to a web site or computer network. It is also the primary means by which the user of a device is identified. However if username/password combinations are not kept confidential, the security and integrity of the network can be compromised.

- Ensure that each person requiring access to the school network is assigned a unique username and password and that they understand that they are not to be shared with anyone else, including the IS team.
- Discuss with your IS team the possibility of using *passphrases* or *strong passwords*:

1.3. Content Filters

Ensure that Internet access is controlled by a content filter, but be aware of their limitations. Content filters are merely software programs implementing someone else's subjective judgement, they typically block access using keywords, URLs or IP addresses which can lead to over-blocking or under-blocking, they will not provide protection against cyber-bullying or stalking and they are incapable of determining if an attempted access was deliberate, a mistake or the computer acting independently of the user. (Ayre 2001, Heins, Cho & Feldman 2006, Houghton-Jan 2008, Hunter 2000, Schneider 1998, Schrader 1998).

- Consider having the content filter software notify the user of the attempted inappropriate access and give them the option of:
 - i. Continuing but having the request logged,
 - ii. Abandoning the request or
 - iii. Asking for a management review of the block.

Just logging the web request without any involvement by the user means there is no opportunity for them to express concern about web accesses they did not initiate.

- If the user is not notified of attempted inappropriate accesses:
 - i. Discuss any inappropriate site accesses with the user.
 - ii. Pay particular attention to the time and pattern of accesses.
 - Was the user present when each access occurred?
If not, other users or Trojan activity may be responsible.

1.4. The Forensic Analysis

It is possible that a school may need to formally investigate an individual suspected of inappropriate behaviour with their IS equipment. It is vitally important that this investigation is carried out correctly, otherwise valuable evidence can be inadvertently destroyed. Such evidence is the key means by which the subjects innocence can be proved (or otherwise). It must be remembered at all times that the subject of the investigation has a right to a fair investigation.

Typically a forensic analysis is conducted by a Computer Forensics company at the request of the principal or Board of Trustees. It is also the activity which presents the biggest threat to the accused if the objective is simply to locate corroborating evidence instead of determining exactly what happened.

To protect all parties involved in a forensic examination a number of steps should be taken: (Sanderson 2008)

1. DONT PANIC!!!
2. Do not presume that you already know what has occurred.
3. Treat the investigation as if it were a crime scene. If you do not have anyone trained as a first responder, call in a computer forensics firm. The people who perform the forensic analysis should be certified or suitably qualified professionals who are aware of the correct procedures for conducting a forensic examination
4. Work with the forensics company to make a plan for dealing with the issue. Work the plan methodically and without haste.
5. Until the forensics company arrives, the target machine should be secured and protected. You should not interact with it in any way (i.e. if the machine is running, leave it running until the forensics team arrives. If it is turned off, leave it off). Do not run any programmes, analysis or otherwise. This includes using remote-control software (e.g. VNC).
6. Have the forensics company:
 - Make a forensically-sound (verifiable, exact) duplicate of the media on machine being examined
 - Confirm that the material in question exists on the machine being examined
 - Provide a timeline and detailed explanation of how the material arrived on the machine.
7. Ensure that no information is released to the public or media until a full investigation has taken place. If the community gets a hint that some impropriety has occurred, you will have parents calling for staff dismissals and threatening to withdraw their children from the school.

If is very easy to get into a position where the guilt of the accused is assumed and subsequent actions then reinforce that opinion. However, if they have done nothing wrong, a lot of damage can be done to the individual and the school if the situation is not handled properly.

1. Stick to the facts. If the evidence does not support the idea that the accused has done something wrong, bring the investigation to an end before it gets out of control.
2. Limit any conclusions to those that can be supported by the forensic evidence and avoid the temptation to be sensationalist. E.g. If you decide to include some of the offending material in the forensic report, limit it to a representative sample. Reproducing thousands of pornographic images in a forensic report may be useful for generating an emotional response, but it does nothing to explain how the material arrived on the computer or to prove that the accused put it there.
3. In New Zealand, no funding is available for teachers to defend themselves against accusations of impropriety, whereas the School and NZTC have considerable funds at their disposal. So in all fairness, keep the costs to the accused to a minimum and consider reimbursing them if no fault is found.
4. Get a trained individual to perform some initial checks (on the duplicate drive) to see if it is simply a malware infestation
 - Does a virus scan of the duplicated media reveal any viruses or Trojans (i.e. malware) that might explain the inappropriate content?
 - Was the person physically present at the times the inappropriate files were created?
5. Provide the evidence to the accused in a timely manner and an easily accessible format. e.g. providing them with an EnCase image of the hard drive is only useful in the unlikely event that they own a copy of EnCase.

The evidence might include such items as:

- Details of how the drive was handled, copied and analysed.
 - The full EnCase report, including the filters and conditions used.
 - A list of the active processes (displayed and hidden) that were running on the machine when it was seized.
 - A printout of the NT security logs.
 - A copy of the hard drive (or clone).and hash validation document.
 - Details of the network configuration, including the content filtering and anti-virus software in use.
6. Do not go looking for *additional* evidence to use against the accused. Any old hard drives and backups are unlikely to have been properly secured, so are of minimal value, and every additional piece of information that has to be reviewed, extends the time and expense for everybody.

[Tami Loehr referring to the North Short Principal incident]

The initial work that was done was sloppy and incomplete, so they are doing sloppy and incomplete work before they decide to convict. Well... that's not fair. Why don't you do your work, ahead of time, and let this guy live his life and then when you've decided 'maybe it wasn't him', then he isn't affected by it. But instead, they are jumping in, ruining his life, and then they come back later after someone has had to pay for this additional forensic examination with 'Oh OK, well we're sorry'. Loehr, T. (2008)

2. The Teacher's Responsibility

In this section, some suggestions are made on how teachers (and other educators such as principals, teacher support staff etc) can minimise their risk profile when using a school network or the Internet. It also gives recommendations on how to handle a forensic examination following a computer-related incident.

An issue which is often overlooked is that educators are not information technology experts, so they rarely encounter the harder aspects of computing (Segal 2004). This means they tend to view computers and the Internet as simply being a means to an end and so only learn enough to allow them to perform their daily tasks, but little more. Unfortunately, when dealing with the Internet, this is akin to sending them into a Wild West gunfight armed with a water-pistol.


“...The [House of Lords Science and Technology Committee] report said that it was no longer realistic to expect individuals to be responsible for their own security because the criminals were too sophisticated and could “outfox” them.

Ford (2007)

It issued a stark warning: “The internet is now increasingly the playground of criminals. Where a decade ago the public perception of the e-criminal was of a lonely hacker searching for attention, today’s ‘bad guys’ belong to organised crime groups, are highly skillful, specialised and focused on profit.”

Ford (2007)

2.1. Desktop

- Desktop computers and laptops should be secured when they are left unattended. There are a number of ways to achieve this, but the easiest is to hold down the Windows Key  whilst pressing L (Lock) on a Microsoft Keyboard

2.2. Passwords

- Passwords should not be shared with anyone (including the IS team) and they should be changed every 3-4 months. The IS team should also be notified if a caller or email requests their sign-on details as this may indicate a phishing or social-engineering attempt.
- Use *passphrases* or *strong passwords*:
- Do not use of easily guessed passwords such as names of family members, friend's names or famous people, sports teams, hobbies, pets, etc.
- Use a combination of upper and lower case letters, and numbers.
- Use a different password for each system that must be accessed.

2.3. Avoid Adware and Spyware

Spyware and Adware can put the school's network at risk, produce unwelcome pop-ups and make unauthorised changes to your machine.

“Adware is software that generates revenue from advertising targeted at the user of the computer where the software resides. It earns revenue either for the vendor or for the vendor's partners. Adware installs itself on a user's machine-often as the trade-off for a piece of 'free' software. A PC infected with adware can be plagued by constant pop-up promotions and the slowing down of the computer's speed. If at all possible, adware websites should be avoided.”
McAfee (2009)

“Spyware is a program that monitors and gathers user information for different purposes. Spyware programs usually run in the background, with their activities transparent to most users. Many users inadvertently agree to install spyware by accepting the End User License Agreement (EULA) on certain free software.”
TrendMicro (2009)

- Do not install any software on the computer yourself. Instead, submit a request to the IS team who have the skills to vet the software and correctly install it.
- Do not trust unexpected emails with attachments even if they look like they come from someone you know. If in doubt, delete it !
- Never attempt to dismiss any pop-up windows that have 'close' or 'X' buttons inside the window. Only ever use the operating system's close button in the upper right corner of the window frame. (Riley 2009)

2.4. Be Aware of Phishing

Phishing emails attempt to trick the recipient into divulging information that may be useful to the sender. This is a problem in a school environment, where the release of sign-on details could compromise the schools network or lead to the release of confidential information.

“Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.”
Wikipedia (2009)

- Be suspicious of e-mails that try to scare, or compel you, to act quickly to prevent an account closure, correct a security problem, to validate your personal details or to collect prize money.
- Phishing emails are usually produced in bulk, so will tend to lack specific details such as your full name, or account details. Instead they will use generic terms such as “valued customer”, “dear friend” or “your account”.
- Do not click on any links or fill in any forms provided by a suspicious email. If you need to go to the organisation mentioned in the email, type the web address of the organisation directly into the browser's address bar – do not copy-and-paste the address from the email.

- If an email takes you to a web site, be wary because it may send you to a spoofed (fraudulent) version of the website. Sometimes you can tell by looking at the website, but even that is not foolproof and can sometimes be misleading.
- If you believe you have received a phishing email, check out web sites such as <http://www.hoax-slayer.com/phisher-scams.html> to see if it's a known scam or locate the company's phone number in the white/yellow pages and ring them.
- If you have received a phishing email, notify the IS team, as the email may have gone to other teachers in the school as well.
- If you believe that you have been deceived (hooked) by a phishing attempt, contact the genuine company by phone and inform them of the mistake. They may have to cancel the credit cards or accounts used in the transaction and change any passwords that were used.
- One of the better safeguards against phishing attacks is common sense:
 - Remember: If It sounds too good to be true, it probably is.
 - Banks typically have large call centres, so they are highly unlikely to resort to emails to confirm account information.
 - How likely is it that a complete stranger has chosen *you* to help move millions of dollars around the world.
 - If you have never paid for a lottery ticket, why would you then expect to win?

2.5. Electronic Communications

Email and social-networking open up a whole new avenue of communications, but they also present their own risks:

- The Internet never forgets:

The things you publish on the Internet are likely to be available to search engines for decades to come and even when you think they are gone, some items can still be retrieved from sites like the *Wayback Machine* at <http://www.archive.org>.

As a general rule-of-thumb, ask yourself if you would be happy for the photos, personal information or comments, you have placed on a social networking site or dating site, to be available to your employer, parents, children, peers or students.

Regularly search the Internet for your name (e.g. "Jane Smith"), nickname and email address to determine what information the Internet holds about you. If you find anything that is incorrect or unsavoury, contact the web site owner and ask for it to be changed or removed.

- Learn email netiquette:

Your school may provide some email rules you should adhere to. If not, use some of the guidelines listed below:

- Do not type your message ALL IN CAPS as it means you are shouting.
- If you are sending an email to a group of people, utilise the BCC (blind carbon) option so that you do not distribute the entire mailing list to everyone.
- Be wary of using 'reply to all'. It is unlikely that *everyone* will benefit from your reply, so only reply to those people who really need a response.
- Reread your email carefully before sending it. If there is any possibility that it may be misunderstood, adjust it to make the message clearer.
- When responding to questions, quote the specific questions you are providing answers for instead of sending the entire message back.
- Provide a SUBJECT line that describes the content of the email.
- Do not send or forward emails that may cause offense.
- Spell-check the email before sending it.

- Do not forward chain letters:

You may receive an email telling you about a new virus, a dying child who is collecting birthday cards or a company giving away free mobile phones or laptops, *do not* forward the email to anyone else.

- Unless it was sent by your own IS team, ignore virus warnings that arrive by email. Anti-virus-software vendors typically distribute their updates via their web sites, so there is no need for them to use email.
- Do not forward emails which others may consider spam unless you absolutely know they are genuine and will be of interest to the recipient.
- Do not participate in email petitions. The petitions are of questionable value as many of the petitions are bogus (e.g. "bonsai kittens") and the intended recipient of the petition cannot know for sure that the names are from genuine, willing participants.
- If you suspect the email you received may be a hoax, run a Google search to see if it appears on one of the Internet-scam information sites (e.g. www.snopes.com, www.hoax-slayer.com, www.hoaxbusters.org, etc).

2.6. Usage agreements

- Most school *Internet and Network Use Agreements* require the teachers and students to agree to a level of conduct when using school equipment. However, the agreements tend to focus on the obligations, responsibilities and consequences of the users, but lack any statement as to what the school's obligations and responsibilities will be in the event that the school's infrastructure fails to perform. Further discussion may be required with the appropriate agencies if this discrepancy is ever to be resolved.

- If the your *Network and Internet Use Agreement* offers you the opportunity to get additional training in order to safely administer and utilise the school's computer network, accept the offer. Continue receiving additional training until you are satisfied that you can fulfil the requirements of the agreement.

2.7. Inappropriate Content

- It's possible you may come across inappropriate content inadvertently during your use of IS system. For example an search the internet for an innocent word or phrase could lead you to an inappropriate webpage, although search engines are getting better at preventing this from happening. For this reason it is sensible to enable 'safe search' settings which are available on all the main search engines
- It is a mistake simply to turn a blind eye and ignore inappropriate material (whether that be images or text) if they appear on your computer screen. Instead you should take appropriate action so you can avoid any future misunderstanding about how the material arrived on your computer.

- If an inappropriate image appears on your computer screen:

One off images may appear on occasions and there is little you can do to stop them, particularly if they arrive from a normal (i.e. non-pornographic) site. However, reporting the incident gives the school the opportunity to block the image and services to explain why it was received.

- Do not dismiss it lightly
 - Send an email to the IS team to tell them what you were doing, what appeared on your screen and whether the visit to the site was accidental (e.g. wrong URL entered), outside of your control (e.g. a redirect from one web site to another one) or a deliberate (albeit perhaps mistaken) access.
 - Retain copies of the emails you sent regarding the incident and any responses received.
 - Log the incident in your school's *ICT Incident Book* if required
- If a porn-storm occurs:
Sometimes opening a webpage or clicking on an image triggers multiple new windows to pop up, one after the other until eventually the screen is covered with these new windows. Usually these new windows contain images which are adverts for porn sites and so this is known as a 'Porn Storm'.

Porn-storms are a real problem. They can be extremely hard to stop and they effectively disable your browser until the porn-storm has run its course. They may also try to trick you into clicking a button which will download malware to your computer.

- Turn off the screen (NOT the computer)
- Contact the IS team and ask them to deal with the problem immediately
- Send the IS team an email asking them for an explanation of the cause and what was done to prevent it happening in the future. Do not accept a verbal response – it must be in writing.
- Retain copies of the emails you sent and any responses received.
- Log the incident in your school's *ICT Incident Book* if required
- Ask the IS team to clear the browser cache or teach you how to do it.

- If illegal material appears on the screen of your computer (e.g. kiddie-porn):

Illegal material appearing on your screen is extremely serious as *technically* you have downloaded the material to your computer and so can be fined \$50,000 or given 5 years in prison. The Department of Internal Affairs (DIA) are not after people who accidentally go to the wrong web site, they are after people who are trading in or collecting illegal material (Netsafe 2008e).

Therefore, if you come across illegal material online you **MUST** report it and you **MUST** make sure the proper processes are followed by your IS department to remove the material from your computer. This is particularly the case for images which depict scenes of child abuse (often referred to as 'kiddie-porn' or 'child porn').

Your actions and the record of events must clearly demonstrate a disdain for the illicit material and an adherence to the school's procedures for dealing with it. You should therefore:

- Contact the IS team and ask them to deal with the problem.
 - Send a follow up email to the IS team to tell them what you were doing, what appeared on your screen and whether the visit to the site was accidental (e.g. wrong URL entered), outside of your control (e.g. a redirect from your site to another one) or deliberate.
 - Also ask them to perform a *permanent delete* of the offending material and to confirm in writing to you that it has been done.
 - Retain copies of the emails you sent regarding the incident and any responses received.
 - Log the incident in your school's *ICT Incident Book* if required
- You might not see everything your computer downloads
 - Sometimes web sites download images to your computer that you won't actually see. These images, which may or may not appear in the browser window, are usually pre-loaded by the web site or browser to improve the performance of the webpage.
 - This means a large number of images can be loaded on to your computer (in a place called the 'browser cache') without any of it ever having being seen. This is even more so where "web accelerator" software is installed, as any web pages the accelerator anticipates may be visited, will also be download automatically (regardless of their content). The extra pages may include pages from web sites the current site links to, but which may never be visited.

- Unscrupulous web sites can deliberately hide images if they wish, perhaps as a way of improving their search engine position or as a way artificially increasing visitor traffic for advertising purposes. A demonstration of how easily this can be done can be found at <http://browserdangers.in-host.net>
- In fact, you don't even need to visit a website for material to be loaded on to your computer without your knowledge. If your computer is infected with 'malware' such as spyware, adware and viruses on your computer could be accessing the internet without you knowing.
- Therefore, if you are accused of accessing inappropriate material or it is found on your computer, it is essential that you ensure a proper forensic analysis is performed to find out how it got there. It might be that your computer is infected with malware, or you have visited a website which inadvertently loaded the content on to your computer.
- A proper investigation will uncover the facts and be able to give a fair and unbiased indication of whether your access was deliberate or as a result of some other factor.
- The rest of this section looks at what you should do to ensure a 'fair trial' if you are accused of accessing inappropriate material.

2.8. Suspicion is conviction

"Porn also has the added benefit of carrying a social stigma that will ensure the accused employee will probably leave without making a fuss. You might be tempted to fight an accusation of an over-enthusiastic expenses claim but only the bravest soul is going to enter into an extended legal tussle over porn. Internet pornography carries a malignant association and significance all of its own, partly because recent child pornography cases have inextricably linked Internet pornography with child pornography in a lot of people's minds."

(Donoghue 2004)

"To think that it is possible for the average layperson to understand all the ins and outs of how a computer works is just not reasonable. What's worse, our employer's don't know any more than we do, and they rely on us to identify problems when they happen. If you are lucky, your employer will know what to do when a crisis happens with your system. If not you'll end up like Julie [Amero], arrested, ridiculed, demeaned and left with useless teacher's degree in special education." – Wes Amero

(Robertson 2007)

- When someone in the academic community is accused of accessing inappropriate material, a strange but unfortunate phenomenon occurs:
 - They will quickly discover who their real friends are.
 - Their past reputation and performance will count for nothing.
 - Innocent past actions will be re-interpreted in the light of the accusations.
 - If the accusation is released to the media, pressure will be applied to have them suspended or dismissed.
 - The school and education sector will focus on protecting the school and cleaning up the *mess* as quickly as possible.

- Some of their peers will do everything within their power to *deal* with the person who has betrayed their profession. This is especially true if the accused had previously held a high-profile position or promoted unpopular ideas.

The risk is that the desire to deal with the issue quickly and cleanly may lead to the accused being treated unfairly, leading to them being wrongfully disciplined or dismissed. This is made more likely when technology is involved because few people have encountered the harder aspects of computing (Segal 2003, Kettinger & Lee 2002) and so have neither the knowledge nor experience to properly assess the situation.

2.9. The Forensic Analysis

The level of understanding of networking and Internet in New Zealand schools, combined with the lack of financial assistance for teachers under investigation can mean that teachers are at a serious disadvantage during an investigation period. It is important therefore that the educator acts wisely to ensure that they do not make their situation worse. You should therefore:

- Have your lawyer present at all meetings
 - You are entitled to have a support person present at any meeting. This is especially important in the early stages of an investigation before the full facts are known to ensure you are being treated fairly.
 - People who have taken proper advice before being forced into an irretrievable position are in a better position to defend false accusations.
- Be careful about “deals”

The school may offer a way out of the situation where the accused takes responsibility for the inappropriate material in exchange for the situation being kept under wraps and handled internally.

 - If you have done nothing wrong, do not feel pressured to make any deals.
 - In the school environment, confidentiality agreements are very difficult to enforce and once it's leaked to the media it's too late.
- Use your own experts
 - If the school has used a forensics company or internal staff to investigate the evidence, You may wish to consider commissioning your own independent forensic investigation in parallel to the school's
 - Do not accept the school's expert advice as being the final answer – they may be wrong.
- Stick to the facts
 - Do not offer the investigators any additional information they have not asked for. If you are under suspicion, even the most casual of remarks, can be misinterpreted and may make your position harder to defend.
 - Keep a full record of all meetings and communications so you can check back what was said and ensure the school is keeping to the correct process.

3. The School Network

In this section, some suggestions are made on how to make a school network more secure, protect networks users from basic mistakes and on how to handle a computer-related incident.


Unfortunately, School IS teams are in an unenviable position. They are often underfunded and understaffed, but are still expected to provide a safe computing environment for teachers and students, whilst protecting their systems from both internal and external attacks. They also need to ensure that in the event of a computer-related incident, they do not change any of the evidence; they must remain impartial and also do their best to assist the first responder and/or computer forensics company.

The following section is aimed at I.S teams and should be used as a checklist to ensure you are following best practice to help you to help your users.

3.1. Operating System

- Ensure that the network and PC's are kept up to date with all security related patches.
- Install antivirus and anti-spyware software and keep them up to date
- Install a personal firewall on laptops so that they are protected when operating outside the school network.
- Enable network security logs and retain them in case they are required for forensic purposes. (Mitnick 2006)

3.2. Desktop

- Encourage the users to lock their computers when they leave them unattended.
 - Using the -L (Lock) combination on a Microsoft Keyboard
 - Using a *LockWorkStation* shortcut created on the desktop
 - Install a screen saver that locks the computer when it is idle
- If computers are allocated to individuals (i.e. not shared), provide machines that have been completely rebuilt from scratch. Allocating a machine previously used by someone else, but not thoroughly cleaned, may save time for the IS team, but it also presents the new user with content they had no part in producing, but may later be held responsible for.
- Use a safe delete utility to *permanently* delete files from a computer when this is required as part of a proper cleanup process. This ensures that the teachers are not held accountable for files they have specifically asked to be erased.

3.3. Security Tweaks

- Do not allow any user account to operate with Administrator rights.
- Disable AUTORUN on Audio CDs and USB Drives (KB967715 2009): Whilst the AUTORUN feature is useful for allowing removable media to automatically run when it is plugged in, it can also be exploited to spread malware.
- Do not allow users to install any software on their machines. Instead, have them submit a request to the IS team who can then vet the software before installing it.
- Configure the system so that the user can see the file extensions on filenames and email-attachments. If they cannot see the extension, they cannot tell whether they are clicking on an MSWord (.DOC) file or an executable (.EXE).
- Centrally manage anti-virus and firewall software. This will give the network administrator oversight of updates, malware activity and status.
- Configure each computer to receive automatic updates from Microsoft.
- Ensure the school's internal domain name space is not a real-world address². This will prevent it from being vulnerable to the WPAD flaw (Fontana 2007).
- Consider using a custom HOSTS³ or PAC file to redirect ad-servers, porn-servers and web tracking links to a non-existent local address (Canter 2004).

3.4. Passwords

- Assign each person requiring access to the school network a unique username and password.
- Ensure that principals and teachers understand that their passwords should not be shared with anyone (including the IS team) and they should be changed every 3-4 months. Enable this as an automatic function if the network permits it.
- If passwords are written down, they should be obfuscated slightly to make them useless to anyone finding the list. e.g. swap some of the characters around, add or omit characters or hide the password characters amongst other characters.
- If users have difficulty remembering complex passwords, it is better for them to write them down and keep them in their wallet/purse than write it on a piece of paper and put it in their desk or under their mouse mat. (Leyden 2005).
- If the idea of storing passwords in a wallet is a bit disconcerting, provide the teachers with a password management utility such as KeePass or Password-Safe.
- Ideally, they should use a different password for each system they need to access.
- Investigate the use of secure key tokens as part of the login process.

² e.g. *someplace.school.nz* is a real-world domain name, whereas *someplace.local* is not.

³ Also refer: <http://www.mvps.org/winhelp2002/hosts.htm>

3.5. Email Clients

- Filter out any emails with attachments that have more than one file extension (e.g. TXT.VBS) or which have a file extension capable of carrying a virus (e.g. EXE, COM, PIF, VBS, BAT etc). (Sophos 2010)
- Turn off the message preview feature / auto-open features in the mail client to prevent unsafe content being displayed to the user.
- Configure the email client to display messages in text format until the senders address is confirmed as being safe.

Note: these precautions are not necessary for the current versions of Microsoft Outlook and Windows Live Mail.

3.6. Content Filters

Discuss the use of content filters with the school's administrators and staff and decide on a model which is appropriate for your particular school.

- Ensure that the software displays a 'content blocked' notification if the user attempts to access inappropriate sites.
- If a user shows repeat access attempts to blocked content, follow up the notifications with a meeting to discuss the attempted accesses.
- Pay particular attention to the time and pattern of accesses. i.e. Was the user present when each access occurred? If not, other users or Trojan activity may be the cause.
- Add any unsavoury sites reported by the principal or teachers to the blocked sites list and confirm to them that the addition has been made.
- If a laptop is being used, enable *web content filtering* security settings in the browser.

Internet Explorer 8	Firefox 3
<ul style="list-style-type: none">▪ Select <i>Tools</i> from the menu bar▪ Select <i>Internet Options...</i>▪ Click on the <i>Content</i> tab▪ Click the <i>Enable...</i> button in the <i>Content Advisor</i> section▪ Set the levels of acceptable web content required	<ul style="list-style-type: none">▪ Download a <i>parental controls</i> add-in from https://addons.mozilla.org/en-US/firefox/search?q=parental+control&cat=all&as=true&vfuz=true&appid=1&lver=any&hver=any&atype=0&pid=0&lup=&pp=100&sort=

3.7. Malware

If a virus or Trojan infects a machine, despite the presence of a virus checker, the machine should be removed from the network (and assuming it is not required for evidential purposes), the hard drive should be cleared using a secure disk eraser and the operating system and applications should be reloaded. (Johansson 2004a, 2004b).

While this may seem a bit extreme, the aim is to address two potential problems:

- As the malware was not detected by the virus checker, the virus checker may have been compromised, so it can no longer be trusted.

“You can be 100% certain that there is no malware you can detect, but you cannot be 100% certain that there is no malware at all.

(Riley 2008)

- The Trojan could have made any changes it wished when it was active on the computer, so there is no way of knowing for sure what damage would have been done and what backdoors may have been installed. Cleaning and rebuilding the system ensures that any changes, inappropriate material or malware downloaded by the Trojan are removed.

“There is no way to tell how the malware has modified your computer beyond the rogue executables you or your antivirus program has found. There is no antivirus removal program that can be guaranteed to have completely cleaned your machine.”

(Grimes 2009)

If the hard drive is required for evidential purposes as part of an investigation, it should be replaced with a clean drive and the original kept in a secure location until it is forensically analysed.

3.8. Manage the Browser Cache

One of the problems teachers face when using the Internet, is that they have little-to-no control over what gets loaded into their browser cache. So over a number of months, a large number of images can collect in their browser cache, which they are totally unaware of and will have a lot of difficulty explaining.

To address this concern, set up the system to so that only a small browser cache is used:

Internet Explorer 8	Firefox 3
<ul style="list-style-type: none"> ▪ Select <i>Tools</i> from the menu bar ▪ Select <i>Internet Options...</i> ▪ Click on the <i>General</i> tab ▪ Click <i>Settings</i> under the <i>Browsing History</i> section ▪ Change the <i>Disk Space to Use</i> setting to 10Mbs 	<ul style="list-style-type: none"> ▪ Select <i>Tools</i> from the menu bar ▪ Select <i>Options...</i> ▪ Click the <i>Advanced</i> Icon... ▪ Select the <i>Network</i> tab ▪ Change the <i>Use up to xx MB of space for the cache</i> to 10

Note that reducing the browser cache to its minimum will not hide the forensic evidence of inappropriate web accesses, but it will ensure that the cache is regularly overwritten and strongly suggests that the cache is not being used as a porn repository.

4. Conclusion

- This paper provides a number of ways that schools, teachers and educators can limit the risks of access to inappropriate content. It seeks to raise awareness of the issues but we can never remove the problem completely. Instead it seeks to provide a balance between the rights of teachers, the usability of computers systems and, of course, the protection of our children.
- In his 2002 paper, Dr John Hope expressed concern at the poor funding of primary school ICT programs and the difficulties schools face providing safe Internet access for their students. Unfortunately, very little has changed since then.
- For anything to improve, more work is required on the part of the education sector and technology groups (e.g. the New Zealand Computer Society), to develop training and resources that will help educators to use technology safely and effectively.
- Additional work also needs to be done on the procedures employed by schools for investigating accusations of inappropriate computer use. The current model puts educators at a serious disadvantage due to the assumption of guilt, being contrary to the principle of natural justice, which is the absolute basis of our legal system.
- This paper attempts to provide advice to schools, teachers and school IS teams to help them manage their user of computer facilities and to ensure that accused teachers have the appropriate opportunity to prove their innocence. It also means that schools can be confident that they have followed the right steps in the event that a teacher has been genuinely accessing inappropriate content.
- One of the key messages in this paper has been the need for a deeper and more substantial forensic analysis when a teacher or principal is accused of accessing inappropriate material. School IS departments are simply not equipped for this type of investigation, and it is arguable whether they need to be. Independent forensic advice is not a cheap option and the question of who funds an investigation still remains.
- It is hoped that the recommendations from this paper are adopted by the Education Sector, with support from the Technology Sector to make our schools a safe place to work and study.

5. Glossary

Malware	Malware is software that is designed to surreptitiously install itself onto a computer without the owners knowledge or informed consent. The term malware is short for <i>malicious software</i> and is general used to refer to hostile, destructive or intrusive software.
Over-blocking	This situation occurs when a filter prevents text or images from being shown, but which should have been allowed through.
Passphrase	A simple easy-to-remember sentence of three to five average-length words. No extra symbols or numbers are necessary. (Riley 2009)
Phishing	Phishing is where a person attempts to acquire sensitive information such as usernames, passwords, account numbers, etc usually via an email appearing to come from a legitimate source.
Social-engineering	Social engineering is where someone attempts to manipulate a person into performing an action or releasing confidential information.
Strong password	A password consisting of a combination of upper and lower case letters, numbers and other characters and is typically a minimum of 8 characters in length.
Trojans	Trojan software is software that is installed for a particular purpose but behind the scenes it is performing other tasks without the owners knowledge or informed consent. Some trojan tricks include 1) opening a back door into the user's computer system, 2) installing other software, 3) stealing passwords and credit card details, and making the users machine a member of a botnet.
Under-blocking	This situation occurs when a filter allows text or images to be shown which should have been blocked.
Viruses	A computer virus is a self replicating computer programs. They tend to be damaging to the machoines they infect and spread via the Internet, or on removable medium such as a floppy disks, CD's, DVD's, or USB devices.
Worms	A computer worm is a self-replicating computer program that uses a network or the Internet to copy itself to other computers. Unlike a virus which is often destructive, the harm caused by worms tends to be limited to bandwidth or processor consumption.

6. References

- Ayre, L. B. (2001). *Internet Filtering Options Analysis - An Interim Report*. Retrieved February 20, 2010, from the State Library of North Carolina: http://statelibrary.ncdcr.gov/hottopic/cipa/InternetFilter_Rev1.pdf
- Canter, S. (2004). *Kill Internet Ads with HOSTS and PAC Files*. Retrieved May 31, 2009, from O'Reilly Windows DevCenter: <http://www.windowsdevcenter.com/lpt/a/4730>
- Donoghue, A. (2004). *Internet porn: Guilty till proven innocent*. Retrieved May 16, 2009, from ZDNet News: http://news.zdnet.com/2100-1009_22-138179.html
- Fontana, J. (2007). *Microsoft Working To Close 8-Year-Old Web Proxy Vulnerability*. Retrieved June 2, 2009, from NETWORKWORLD: <http://www.networkworld.com/news/2007/112607-microsoft-web-proxy-vulnerability.html>
- Ford, R. (2007). *Internet is Becoming as Lawless as the Wild West, Report Peers*. Retrieved May 26, 2009, from The TIMES ONLINE: http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2231564.ece
- Grimes, R. A. (2009). *Starting From Scratch Is The Only Malware Cure*. Retrieved March 1, 2009, from Infoworld - Security Adviser http://weblog.infoworld.com/securityadviser/archives/2009/02/starting_from_s.html
- Heins, M., Cho, C. & Feldman, A. (2006). *Internet Filters - A Public Policy Report*. Retrieved February 20, 2010, from the Free Expression Policy Project: <http://www.fepproject.org/policyreports/filters2.pdf>
- Hope, J. (2002). *Internet Safety: Issues For New Zealand Primary Schools*. Retrieved February 21, 2010, from University of Auckland, Department of Computer Science: <http://www.cs.auckland.ac.nz/~john/NetSafe/Hope.pdf>
- Houghton-Jan, S. (2008). *Internet Filtering Software Tests - Barracudam, CyberPatrol, FilterGate & WebSense*. Retrieved February 20, 2010, from San Jose Public Library: http://www.sjlibrary.org/about/sjpl/commission/agen0208_report.pdf
- Hunter, C. D. (2000). *Internet filter effectiveness—testing over- and underinclusive blocking decisions of four popular web filters*. Retrieved February 21, 2010 from Commission on Online Child Protection (COPA): http://www.copacommission.org/papers/filter_effect.pdf
- Johansson, J. M. (2004a). *Help: I Got Hacked. Now What Do I Do?* Retrieved May 22, 2009, from Microsoft Corporation: [http://technet.microsoft.com/en-nz/library/cc512587\(en-us\).aspx](http://technet.microsoft.com/en-nz/library/cc512587(en-us).aspx)

- Johansson, J. M. (2004b). *Help: I Got Hacked. Now What Do I Do? Part II*
Retrieved May 22, 2009, from Microsoft Corporation:
[http://technet.microsoft.com/en-nz/library/cc512595\(en-us\).aspx](http://technet.microsoft.com/en-nz/library/cc512595(en-us).aspx)
- KB967715 (2009), *Microsoft Knowledge Base Article - 967715. 2009. How to disable the Autorun functionality in Windows.* Last Review: July 29, 2009 - Revision: 4.1. Microsoft Corporation.
- Kettinger, W. J. & Lee, C. C. (2002). *Understanding the IS-user divide in IT innovation*
Communications of the ACM,
Volume 45, Issue 2, February 2002.
- Leyden, J, (2005). *Write Down Your Password Today.*
Retrieved May 21, 2009, from The REGISTER:
http://www.theregister.co.uk/2005/07/19/password_schneier/
- Loehr, T. (2008). *Interview with Tami Loehr by Rob Harley*, December 2008.
3037 West Ina, Suite 121, Tucson, Arizona 85741
Video recording in possession of Rob Harley, Project Melting Pot.
- McAfee (2009). *Adware.* Retrieved May 23, 2009, from McAfee, Inc:
http://www.mcafee.com/us/security_wordbook/adware.html
- Mitnick, K. (2006). *Kevin Mitnick's Security Advice.*
Retrieved May 16, 2009, from W.I.R.E.D:
<http://www.wired.com/science/discoveries/news/2006/11/72116>
- MoE. (1995). *Technology in the New Zealand Curriculum.*
Retrieved August 23, 2008, from Ministry of Education:
<http://www.minedu.govt.nz/~media/MinEdu/Files/EducationSectors/Schools/TechnologyInTheNewZealandCurriculum.pdf>
- MoE. (2004). *Audit reinforces the need for cybersafety in schools.*
Retrieved August 24, 2008, from Ministry of Education - Media Centre:
http://mediacentre.minedu.govt.nz/media-releases/2004/2004_008_1709.html
- MoE. (2008a). *ICT Infrastructure – Security & Cybersafety Policy and Guidelines for Early Childhood Education Services.* Retrieved August 20, 2008, from Ministry of Education: http://www.lead.ece.govt.nz/NR/rdonlyres/E4F1A26D-6234-448E-8E23-2BD94CB4BBE1/0/ECEICTStandardsSecurity_v04.doc
- MoE. (2008b). *The National Administration Guidelines (NAGs).*
Retrieved August 23, 2008, from Ministry of Education:
<http://www.minedu.govt.nz/educationSectors/Schools/PolicyAndStrategy/PlanningReportingRelevantLegislationNEGSAndNAGS/TheNationalAdministrationGuidelinesNAGs.aspx>
- MoE. (2008c). *Primary & Secondary Education - Managed Internet Services for Schools.*
Retrieved August 23, 2008, from Ministry of Education:
<http://www.minedu.govt.nz/educationSectors/Schools/Initiatives/ICTInSchools/ICTInitiativesAndProgrammes/ManagedInternetServicesSolutionsForSchools.aspx>

- MoE. (2008d). *ICT Helpdesk - Hints and Tips*.
Retrieved August 23, 2008, from Ministry of Education:
http://www.tki.org.nz/r/ict/helpdesk/hints_e.php
- Netsafe. (2006a). *Sample Cybersafety Policy and Use Agreements for Personnel of New Zealand ECE Services*. Retrieved May 27, 2008, from NETSAFE.ORG:
http://www.netsafe.org.nz/Doc_Library/download/ECE_Policy_and_Personnel_UA_24_April_260406.doc
- Netsafe. (2008a). *The NetSafe Kit for schools*. Retrieved August 24, 2008, from The Internet Safety Group:
http://www.netsafe.org.nz/keeping_safe.php?pageID=59§ionID=education&menuID=59
- Netsafe. (2008b). *NETSAFE: Hector's World™*.
Retrieved August 24, 2008, from The Internet Safety Group:
http://www.netsafe.org.nz/keeping_safe.php?pageID=206§ionID=education&menuID=206
- Netsafe. (2008c). *NETSAFE: NetBasics*. Retrieved August 24, 2008, from NetBasics:
<http://www.netbasics.org.nz/>
- Netsafe. (2008d). *NETSAFE: Creating Cybersafety Use Agreements*.
Retrieved August 24, 2008, from The Internet Safety Group:
<http://www.cybersafety.org.nz/kit/Use%20Agreements/index.html>
- Netsafe. (2008e). *NETSAFE: Information about Legal and Illegal Pornography*.
Retrieved February 8, 2010, from The Internet Safety Group:
http://www.netsafe.org.nz/archive/legal/legal_default.html
- Panchamb. (2002). *Why Software Systems Fail*. Planet Papers. Retrieved May 16, 2009, from Planetpapers: <http://www.planetpapers.com/Assets/1931.php>
- Riley, S. (2008). *SEC305 - Virtualization and Security: What Does It Mean for Me?* Microsoft Tech Ed 2008. Auckland, New Zealand. September 1, 2008.
- Riley, S. (2009). *Email re: Problems in the NZ Education Sector*. August 1, 2009.
- Robertson, G. (2007). *Porn Pop-Up Teacher Gets New Attorney, PC World Outs Juror*. Retrieved May 16, 2009, from DownloadSquad:
<http://www.downloadsquad.com/2007/02/23/porn-pop-up-teacher-gets-new-attorney-pc-world-outs-juror/>
- Sanderson. (2008). *Resources: Do's and Don'ts*.
Retrieved May 16, 2009, from Sanderson Forensics Ltd:
<http://www.sandersonforensics.com/content.asp?page=12>
- Schneider, K. G. (1998). *Figuring Out Filters - A Quick Guide to Help Demystify Them*. Retrieved February 20, 2010, from SchoolLibraryJournal.com:
<http://www.schoollibraryjournal.com/index.asp?layout=articlePrint&articleID=CA152981>

- Schrader, A. M. (1998). *In Search of the Perfect Filter. Indexing Theory Implications for Internet Blocking and rating Software Products*. Retrieved February 20, 2010, from Canadian Association for Information Science: http://www.cais-acsi.ca/proceedings/1998/Schrader_1998.pdf
- Scoop (2004). *Audit Reinforces The Need For Cybersafety*. Retrieved May 23, 2009, from SCOOP Education Independent News: <http://www.scoop.co.nz/stories/ED0409/S00074.htm>
- Segal, J. (2003). *Professional end-user development and software development methodologies*. Faculty of Mathematics and Computing, Computing Department, The Open University, Walton Hall, Milton Keynes MK7 6AA Retrieved 29th July 2003 from <http://www.co.umist.ac.uk/EUD-net/documents/EUDSegal.doc>
- Segal, J. (2004). *Professional end user developers and software development knowledge*. Retrieved May 18, 2009, from <http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=59337DF01167F1F7D9B8924C5B656AF3?doi=10.1.1.107.4916&rep=rep1&type=pdf>
- Sophos (2010). *Simple steps to defend against viruses, spyware and adware*. Retrieved March 7, 2010, from Sophos Plc: <http://www.sophos.com/security/best-practice/viruses.html>
- TrendMicro (2009). *Glossary – Spyware*. Retrieved May 23, 2009, from Trend Micro Incorporated: <http://us.trendmicro.com/us/threats/enterprise/glossary/s/spyware/index.php>
- Wikipedia (2009). *Phishing*. Retrieved May 29, 2009, from Wikipedia - The Free Encyclopedia: <http://en.wikipedia.org/wiki/Phishing>

Appendix A – MoE Initiatives

The Ministry of Education aims to provide quality ICT programmes in New Zealand schools through a number of initiatives:

The Ministry of Education's *technology curriculum* (MoE, 1995) aims to help students to gain a level of technological literacy through the development of:

- knowledge and understanding of technology;
- technological capability;
- Understanding of the role of technology in society.

The curriculum also requires that this should occur in a safe and secure environment (MoE, 2008a, 2008b) by:

- Providing a safe physical and emotional environment for students
- Complying in full with any legislation currently in force or that may be developed to ensure the safety of students and employees
- Protecting children from exposure to material that, may be inappropriate or harmful
- Protecting children from exploitation.

The Education Ministry has participated in, and in some cases funded, a number of Internet Safety Initiatives including:

- Establishing a Help Desk for Schools to act as a first point of contact for Internet concerns and issues (MoE, 2004).
- Arranging managed Internet services, including firewall, content filtering, email filtering, spam protection, and monitoring/reporting tools (MoE, 2008c)
- Providing CA-security anti-virus software to schools at no cost (MoE, 2008d)
- Promoting the use of Netsafe's *Internet Safety Kit for Schools*, *Hector's World™*, *NetBasics* and *Acceptable Use Agreements* (netsafe, 2008a, 2008b, 2008c, 2008d).
- Partially funding audit services to perform drive audits and clean-ups (MoE, 2004)
- Providing extensive information about ICT Infrastructure at their Early Childhood Education site <http://www.lead.ece.govt.nz/ICTInfrastructure/default.htm>.

There are also guidelines for schools on what actions to take in the event that objectionable material or inappropriate behaviour is detected:

- Utilising the *NetSafe Kit for Schools* at <http://cybersafety.org.nz/kit/> (Netsafe, 2008a)
- Enacting the protocol defined in the school's *Internet Use Policy* (Netsafe, 2008a)
- Involving the Department of Internal Affairs (DIA) if it is believed that an educator has committed a censorship offence.

Whilst commendable, these initiatives and guidelines incorrectly assume that the ICT infrastructure is robust and that if anything goes wrong, the problem lies with the educators. However, computer technology often fails to perform to expectations (Panchamb 2002) and the Ministry's own research has confirmed that, despite the best of intentions, providing safe Internet access is extremely hard (Scoop 2004).

Appendix B – News Articles

The Washington Post

Internet Explorer Unsafe for 284 Days in 2006

For a total 284 days in 2006, exploit code for known, unpatched critical flaws in pre-IE7 versions of the browser was publicly available on the Internet. Likewise, there were at least 98 days last year in which no software fixes from Microsoft were available to fix IE flaws that criminals were actively using to steal personal and financial data from users.

http://blog.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html

Watchful Eye Better Than Web Filters

The Australian federal government's Internet filters will be outpaced by the emergence of offensive web pages and won't stop offensive material appearing in email inboxes, according to the internet Society of Australia. Internet Society of Australia president Tony Hill said it is up to parents, not the web filters, to prevent children from being exposed to graphic material.

<http://computerworld.co.nz/news.nsf/news/857EDFE9475118DCCC2575C100737006>

COMPUTERWORLD
The Voice of the ICT Community

BBC NEWS

Google searches web's dark side

One in 10 web pages scrutinised by search giant Google contained malicious code that could infect a user's PC. Researchers from the firm surveyed billions of sites, subjecting 4.5 million pages to "in-depth analysis". About 450,000 were capable of launching so-called "drive-by downloads", sites that install malicious code, such as spyware, without a user's knowledge. A further 700,000 pages were thought to contain code that could compromise a user's computer, the team report.

<http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/6645895.stm>

Nearly All PCs Run Vulnerable Software, Firm Says

A survey of 20,000 computer systems running Microsoft Windows found that nearly all ran at least one program with a vulnerability that put the computer at risk, security firm Secunia said in a brief analysis published on Wednesday. Both responsible researchers and online criminals are increasingly focusing on finding vulnerabilities in third-party applications. Even flaws in security software pose a threat to systems, researchers say.

<http://www.securityfocus.com/brief/867?ref=rss>

Secunia
Stay Secure



Creative Commons License






© Creative Ideas Limited 2009
Some Rights Reserved

Except where otherwise noted, this work is licensed under the
Creative Commons Attribution-NonCommercial-ShareAlike (New Zealand) License 3.0.
<http://creativecommons.org/licenses/by-nc-sa/3.0/nz/>
<http://creativecommons.org/licenses/by-nc-sa/3.0/nz/legalcode>

You are free:

-  **to Share:** to copy, distribute and transmit the work
-  **to Remix:** to adapt the work

Under the following conditions:

-  **Attribution** You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
-  **Non-commercial:** You may not use this work for commercial purposes.
-  **Share Alike:** If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

With the understanding that:






Waiver: Any of the above conditions can be waived if you get permission from the copyright holder.

Other Rights: In no way are any of the following rights affected by the license:

- Your fair dealing or fair use rights;
- The author's moral rights;
- Rights other persons may have either in the work itself or in how the work is used, such as publicity or privacy rights.

Notice — for any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to the web pages listed above.

Contributor BIOS

	<p>Warren Anderson has over 30 years experience in information technology in various roles including IS management, systems architecture, security and application design. He earned a Master of Information Systems (MIS) degree with 1st class honours from Massey University in 2005 and in 2006 he acted as a technical expert representing a North Shore school principal who had been falsely accused of downloading a large volume of inappropriate material. Working closely with the defendant's legal representative, he proved beyond any doubt that the Principal was an innocent victim of a malware attack. Through this case he has direct detailed experience of the technology and process challenges that teachers face when they are under suspicion of inappropriate online behaviour.</p>
	<p>Andrew Hooker is a litigation specialist with extensive experience in insurance and financial services law. He graduating from Auckland University in 1990, and is currently working as a Senior Associate at Turner Hopkins Barristers and Solicitors in Takapuna, Auckland. He has developed a reputation as a passionate advocate for his clients and is regarded as an expert in insurance and fraud throughout New Zealand and the Pacific, so is a sought after speaker for conferences and training events. His work defending the North Shore school principal and others, against charges of inappropriate online behaviour, has given him unique insights and understanding in this area.</p>
	<p>Stephen (Skip) Parker has been involved in the IT community for over 15 years and has gained a wealth of knowledge with some of New Zealand's largest IT environments and International companies such as Geac Computers, Vodafone and HP. He specialises in Internet, security and Communications technologies and his personal interests include internet security with particular attention to intrusion methodologies and history of black-hat / white-hat practitioners. Skip maintains internet services for a large number of non profit social organisations such as Tear Fund New Zealand and Baptist Youth Ministries and has been involved in a number of business matters investigating breaches of company policies with internet usage across a range of different companies. Currently engaged with non profit broadcasters, Skip heads up the Information Technology team at Rhema Broadcasting Group while consulting to a large international affiliation of television and radio stations on emerging internet technologies.</p>
	<p>Steve Riley has over 21 years experience in information technology and earned a BS computer and information science degree from the Ohio State University in 1989. He is currently the Senior Technical Program Manager at Amazon.com and his previous roles included Senior Security Strategist and Senior Consultant Security Practice at Microsoft Corporation. He specialises in Internet standards, protocols, design, and operation, security analysis, assessment, and incident response and is a effective communicator across broad and mixed technical and business audiences.</p>
	<p>Dave Simpson has been involved in the Internet safety arena for nearly 10 years whilst working in the UK Internet industry. He has held the position of vice-chair of the Internet Watch Foundation (IWF) Funding Council, the UK's self regulatory hotline for reporting illegal online content, and was a Director of the UK's Internet Service Provider Association. Prior to moving to New Zealand in 2009 he worked for one of the UK's biggest telecommunications providers and was responsible for broadband regulatory policy. He has worked closely with regulators, governments and law enforcement bodies and was involved in the formation and implementation of the UK 'Byron Review' recommendations.</p>

Acknowledgements

- *Encase* is a trademark of Guidance Software.
- *Firefox* is a trademark of Mozilla Corporation
- *Microsoft, Windows, Windows XP, Windows 2000, Windows Vista and Windows 7* are trademarks of Microsoft Corporation in the United States and other countries.
- *Internet Explorer* is a registered trademark of Microsoft Corporation in the United States and other countries.
- *VNC* is a trademark of RealVNC Limited
- *Wikipedia* is a registered trademark of the Wikimedia Foundation, Inc.