
Internet Access Management

Introduction

A recent survey of New Zealand teenage girls found the following:

- Nearly ¼ felt unsafe or threatened online at some time.
- 1 in 3 had a face-to-face meeting with someone they had contacted online.
- 60% had sent a photo, phone number or address to someone they had contacted online.

Schools worldwide are providing Internet access to more and more young people. It is now being realised that more care must be taken to ensure young people benefit from this access rather than being frightened away.

Overseas experience also shows a risk to institutions by the misuse of computer equipment and Internet access. A number of schools and other learning institutions have been sued for allowing young people to access objectionable material.

The Education Review Office in future will routinely ask schools for their Internet policies and procedures.

Although there is no way to guarantee 100% the complete safety of individuals on the Internet there are a number of precautions that can be taken to ensure the risk and sense of risk is minimised.

Coupled with these rules there are software packages available which are designed to ensure young people are not exposed to anything objectionable while browsing the Internet.

Schools' Liability for Internet Usage

Overseas (particularly in America) a number of schools have been prosecuted for providing unsafe Internet access to students. In New Zealand no court case has yet defined a precedent for this issue.

An opinion from the New Zealand Internet Safety Group says *'If there is an incident of misuse in a school, and the school can demonstrate that they have made a reasonable effort to ensure safety, they will probably not have a problem.'* And *'If there is an incident, and a school is offering students Net access with no policy or procedures in place, they are putting themselves at risk.'*

A further opinion from Rudd Watts & Stone (lawyers) says *'If, for example, it can be shown that a school did not take reasonable precautions to prevent schoolchildren from viewing websites depicting graphic horror, violence or sex, the parents of children who are thereby disturbed or traumatised could bring an action in negligence against the school.'*

From this it is obvious schools need a policy in place to ensure the safety of students, staff and the school. This policy should include Internet usage rules for staff and students, procedures for checking compliance of Internet rules and disciplinary procedures relating to misuse of the Internet resource.

The Internet Safety Group recommend signed contracts be developed for students, parents and staff, to ensure all groups are aware of inappropriate Internet behaviour.

Internet Access Safety Guidelines

'Stranger Danger' is a message that has been drummed into children for a number of years in an attempt to minimise the risks faced by young people. With the Internet now firmly in place an online equivalent is required to provide young people with a list of commonsense guidelines that can be easily followed to minimise any possible risks. These guidelines should include the following:

- Never give out personal information in chat rooms or on websites. This includes information like your surname, phone, address, age, sex, city and school.

- Never arrange a meeting with an individual met online without first discussing the issue with an adult (parent, teacher etc).
- If you feel threatened or intimidated on the Internet tell an adult immediately and leave the site or chat room you are in.

Internet Access Rules

Younger persons should be provided with a clear list of do's and don'ts in relation to Internet access. Penalties for not following rules and procedures should be made known to discourage young people from misusing Internet access.

The rules detailed below are an indication of the type of rules that should be provided to young Internet users:

- Never attempt to gain access to or compromise the security of any other computer connected to the Internet using cracking, hacking or any other technique.
- Never knowingly participate in the spreading of viruses, chain letters or Trojan items.
- Comply with New Zealand and International laws relating to copyright, trademarks, privacy and indecent or obscene material.
- Never knowingly access, store or pass information, data or files that may be offensive to other persons.

Software Options

There are a number of software packages available that can limit sites that are accessible, language that is inappropriate and maintains records of sites visited. The product we recommend is called Cyber Patrol and is recognised as one of the most effective ways of limiting Internet access rights.

Cyber Patrol is designed to run on Microsoft Proxy Server, Novell Borderware or on a local Microsoft Windows 95/98/2000 PC. Cyber Patrol maintains a list of sites not suitable for younger people and downloads these regularly. If a site on the list is accessed the product diverts the Internet browser to a Cyber Patrol screen and prohibits access to the banned site. Cyber Patrol also maintains a list of unacceptable words and can be configured to prohibit these words in chat room sessions.

Marc George

Document copyright © 2001
All Rights Reserved
Technology Solutions – www.techs.co.nz