

Digital Child Exploitation Filtering System

Code of Practice

**A code for the operation of the Department of
Internal Affairs' website filtering system to
prevent access to websites containing images
of child sexual abuse**

AUGUST 2009

CONTENTS

1.	Background	3
2.	The Films, Videos, and Publications Classification Act	3
3.	How the filtering system works	4
4.	The Filtering List	5
4.1	<i>How it's compiled</i>	5
4.2	<i>Where it's located</i>	5
4.3	<i>Review process</i>	5
4.4	<i>Official information</i>	5
5.	The Audit process	6
5.1	<i>Commitment to transparency</i>	6
5.2	<i>Independent Reference Group</i>	6
6.	What happens and what users will see	5
7.	Data	9
7.1	<i>What data is collected?</i>	9
7.2	<i>What is the data is used for</i>	9
8.	What the system won't do	10
9.	Safety message	10
10.	Review of the Code	10

Digital Child Exploitation Filtering System

Code of Practice

1. Background

- 1.1 The expansion of the Internet has led to many positive developments. However, the fact remains that criminals, individuals as well as organised groups, are also using this technology as a means of producing, collecting and distributing images of child sexual abuse.
- 1.2 Child sexual abuse images are not “just images” but evidence of actual criminal activity. The possession and distribution of this material creates an international market that supports and encourages further abuse. The children who are victims of this activity sometimes suffer the psychological effects of their abuse for many years after the physical offending has ended. Images that are distributed on the Internet never go away.
- 1.3 Up until recent years, websites containing child sexual abuse images were very rarely commercial in nature and were motivated by personal gratification and the need to seek out like-minded persons. However, there is a worrying trend in the growth of commercial websites offering password-controlled access for a fee (usually charged to a credit card). These websites can be hosted anywhere in the world making international co-operation all the more crucial when dealing with them.
- 1.4 The Digital Child Exploitation Filtering System is designed to assist in combating the trade in child sexual abuse images by making it more difficult for persons with a sexual interest in children to access that material.
- 1.5 New Zealand law contains no provision that specifically authorises the operation of a website filtering system or to require ISPs¹ to connect to such a system. Participation in the Digital Child Exploitation Filtering System by ISPs is therefore voluntary and this provides an effective means of ensuring that the system keeps to its stated purpose. If ISPs become uncomfortable with the direction of the system, they can withdraw.
- 1.6 The willingness of ISPs to participate in the scheme is a demonstration of New Zealand’s commitment to combating the trade in human misery that is the possession and distribution of child sexual abuse images.

2. The Films, Videos, and Publications Classification Act

- 2.1 The Films, Videos, and Publications Classification Act 1993 (the Act) deems a publication to be objectionable if it promotes or supports, or

¹ Internet Service Provider

tends to promote or support the exploitation of children, or young persons, or both, for sexual purposes (section 3(2)(a)).

2.2 The Act provides that possession of an objectionable publication with knowledge or reason to believe it is objectionable is a serious offence carrying a terms of imprisonment not exceeding 5 years or a fine not exceeding \$50,000.

2.3 The offence of distributing an objectionable publication, including over the Internet, with knowledge that the publication is objectionable carries a maximum term of imprisonment of up to 10 years.

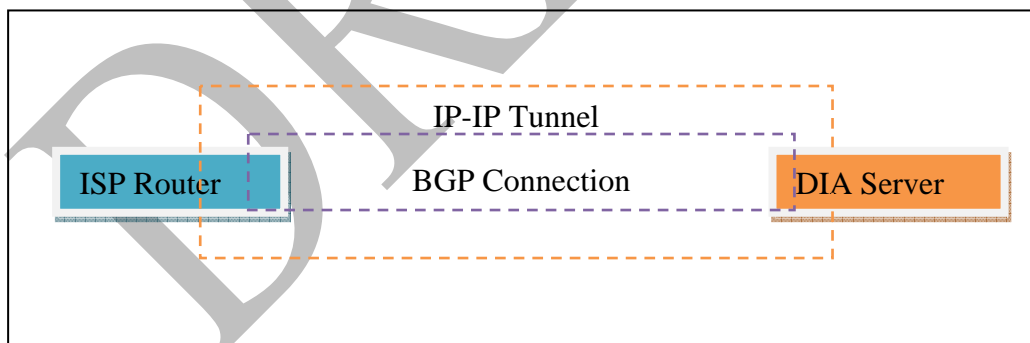
2.4 A person who views a website containing child sexual abuse images is in possession of those images, if only for the period they appear on the screen. The Digital Child Exploitation Filtering System therefore will help prevent inadvertent exposure to these images and will also help prevent New Zealanders from committing crimes.

3. How the filtering system works

3.1 The system designed by Netclean Technologies Sweden AB, filters users requests via Border Gateway Protocol (BGP)² and a master list of known objectionable sites. As a result, it is highly adaptable to websites changing their hosting provider, which is a common step taken by the hosts to avoid detection by law enforcement agencies.

3.2 The connection to a service provider requires 2 steps:

- A dedicated Tunnel is set up between two locations
- A BGP session is then established.



All participant providers will be provided with a common tunnel and BGP session design.

3.3 The filtering list is distributed to ISPs as routing instructions which are added to the ISPs' routing tables with the instruction that any access to those routes needs to come through the Department's system. The method of filtering and the location of the filter on the network has been chosen so that there is no identifiable degradation to the performance of the Internet.

² The Border Gateway Protocol (BGP) is the core routing protocol of the Internet. It maintains a table of IP networks or 'prefixes' which designate network reach ability among autonomous systems (AS).

4. The Filtering List

4.1 *How it's compiled*

4.1.1 Over the last 4 years the Censorship Compliance Unit has developed a large database of sites offering child sexual abuse material. The Unit has become an affiliate of the CIRCAMP³ initiative, which is initiated by the European Chief of Police Task Force and is solely aimed at combating organised criminal groups behind the commercial sexual exploitation of children. These partnerships together with the database already created by the Unit's forensic examination of offenders' computers have enabled the website filtering initiative to filter access to over 7000 sites.

4.1.2 In addition, an online reporting facility for child sexual abuse images has been launched by ECPAT NZ⁴. Called *Child Alert*, it supports the Department's enforcement activity by allowing members of the public to alert the Department to illegal content on the Internet. The hotline enables a fast response for illegal content originating from New Zealand.

4.1.3 The Chief Censor provides expert advice on any matter that requires further clarification. As the filtering list has been compiled so that only sites that are clearly illegal (ie no grey areas) are included, it is not anticipated that the operation of the system will require a high level of participation by the Chief Censor.

4.2 *Where it's located*

The filtering list is retained on a central server in the Department's offices. As the filtering list is distributed to ISP servers in the form of routing instructions, ISPs are not provided with website URLs and the list can be maintained securely.

4.3 *Review process*

4.3.1 The list is reviewed monthly, manually, to ensure that it is up to date and that the possibility of false positives is removed.

4.3.2 Additions are only made to the list with the agreement of at least 3 warranted inspectors of publications that the material on the website meets the criterion that they explicitly show children being sexually abused.

4.3.3 All sites on the list are visited and have a report that identifies the investigating officer and what he or she saw on the site when it was last reviewed.

4.4 *Official information*

4.4.1 The filtering list is official information in terms of the Official Information Act 1982. While this means that members of the public and media may request copies of the list, the Department is strongly

³ COSPOL Internet Related Child Abuse Material Project. COSPOL = Comprehensive, Operational, Strategic Planning for the Police.

⁴ End Child prostitution, Child Pornography and Trafficking in Children.

of the view that there is good reason under the Official Information Act to refuse requests for the list.

- 4.4.2 Persons refused access to the list may seek a review of the Department's decision by the Office of the Ombudsmen.

5. Audit process

5.1 *Commitment to transparency*

The Department considers that continued public support for the operation of the Digital Child Exploitation Filtering System requires that the operation of the system be as open to public scrutiny as possible.

5.2 *Independent Reference Group*

- 5.2.1 The Department will institute an Independent Reference Group (IRG) to maintain oversight of the operation of the Digital Child Exploitation Filtering System to ensure it is operated with integrity and adheres to the principles set down in this Code of Practice.

- 5.2.2 Membership of the IRG, which will meet at least six monthly shall be:

-
-
-
-
-

(Membership to be determined)

- 5.2.3 Reports of the IRG will be published on the Department's website.

6. What happens and what users will see

- 6.1 Once a requester seeks an Internet Protocol (IP) address that is on the filtering list the pre-loaded routing instructions on the ISP's system determine that the quickest route to that address is via the DIA's system.

- 6.2 When the request is received in the DIA's system the particular Uniform Resource Locator (URL) requested is checked against the filtering list. If there is not a match, the request is allowed on its way to the world-wide web.

- 6.3 If there is a match between the requested URL and the filtering list the requester is redirected to a landing page.

- 6.4 The landing page (see below) is designed to achieve the following objectives:

- Inform the requester that he/she has been prevented from accessing the requested website
- Inform the requester of the reason for the redirect
- Provide the requester with a method to appeal the action.

- 6.5 The landing page will also include a link to the Department of Internal Affairs website, where additional information about the operation of the censorship system and help seeking can be found.

**DIGITAL CHILD EXPLOITATION
FILTERING SYSTEM**

STOP!

CONTACT:
EMAIL: INFO@CHILDALEERT.ORG.NZ

REPORT IT
IF YOU HAVE COME ACROSS A WEBSITE THAT YOU THINK IS PROMOTING CHILD ABUSE REPORT IT HERE

 **Child Alert**

→ **ATTENTION:**
YOUR WEB BROWSER HAS ATTEMPTED TO CONTACT AN INTERNET WEBSITE THAT IS USED FOR THE DISTRIBUTION OF IMAGES OF CHILD SEXUAL ABUSE.

THIS ATTEMPT HAS BEEN BLOCKED.

IF YOU HAVE ANY OBJECTIONS TO THIS WEBSITE BEING BLOCKED PLEASE COMPLETE THIS FORM [WEBSITE APPEAL](#) .

FOR FURTHER INFORMATION PLEASE VISIT WWW.DIA.GOV.T.NZ

STOP!

COPYRIGHT © 2007 DCE.NET.NZ

- 6.6 If a requester considers that they have been wrongly blocked from visiting a legitimate website then they can click on the link to the Website Appeal page to fill in an appeal.

STOP!

CONTACT:

EMAIL: INFO@CHILDALERT.ORG.NZ

Note: This form requires cookies to be enabled. For instructions on enabling cookies click [here](#)

Url:

Type verification image:

3749

Reason:

Submit

REPORT IT

IF YOU HAVE COME ACROSS A WEBSITE THAT YOU
THINK IS PROMOTING CHILD ABUSE REPORT IT HERE



- 6.7 The appeals process is designed to follow a set path to ensure privacy of the user making the appeal and also to protect the system from exploitation. The appeals process is anonymous and does not ask for the user's contact details and, because it relies on completing a form on Department's system, it provides no method for identifying the complainant.
- 6.8 Upon a successful signal being sent to the system, the appeal is dispersed to nominated inspectors of publications within the Censorship Compliance Unit for follow up. This follow-up will involve the re-examination of the website concerned to determine whether it still meets the criterion for inclusion on the filtering list (ie. contains images of child sexual abuse).

6.9 The appeals submitted and the actions taken will be reported to the IRG. The reports will be published on the Department's website.

7. Data

7.1 What data is collected?

7.1.1 During the course of the filtering process the Department logs the following information regarding a request for a blocked website:

- Connection Number - relates to the number allocated to an ISP when it is included on the system and the type of connection eg. GIF2.
- Local IP – represents the IP address of the user – this is anonymised to protect the identity of the requester.
- Request - encompasses 2 fields: the Originating Site and the Requested Site.
- Remote IP - relates to the address of the remote site, this uses random numbers to ensure the Department cannot track it back.

7.2 What is the data used for

7.2.1 The collection of this data is necessary so that the system is able to be reviewed to ensure 24-hour 365-day uptime and no loss of business due to a technical glitch or fault, for ISPs who join the system.

7.2.2 The logs are used to troubleshoot the connections between the Department's system and the ISP. As we are providing a service to a commercial organisation, it is our responsibility to ensure that the Department is able to offer the same level of service expected of any commercial enterprise.

7.2.3 As no identifiable information is stored about the user requesting a website, this data cannot be used in support of any investigation or enforcement activity undertaken by the Department. However, the data will be used for statistical and reporting purposes, for example to inform the Department of the level of demand in New Zealand for child sexual abuse images.

7.2.4 The logs will be kept for 30 days, which is the standard period for keeping logs for troubleshooting and is consistent with Rule 9 of the Telecommunications Information Privacy Code 2003. At the end of this period the logs are then manually deleted and a record is made noting this.

8. What the system won't do

- 8.1 The Department of Internal Affairs appreciates that website filtering is only partially effective in combating the trade in child sexual abuse images. In particular website filtering is effective only after the fact and does not prevent the creation of illegal material nor, in the case of images of child sexual abuse, the exploitation of children. The system also will not remove illegal content from its location on the Internet, nor prosecute the creators or intentional consumers of this material.
- 8.2 The Department also acknowledges that website filtering systems are not 100% effective in preventing access to illegal material. A person with a reasonable level of technical skill can use tools that are freely available on the Internet to get around the filters.
- 8.3 As illegal material, such as child sexual abuse images, is most often traded on peer-to-peer networks or chatrooms, which will not be filtered, the Censorship Compliance Unit carries out active investigations in those spaces.

9. Safety Message

- 9.1 It is widely recognised that "content risks" (the harm inflicted by accidentally viewing inappropriate material) are among the least significant of the dangers that children face in an online environment.
- 9.2 The Department is aware that a website filter could give parents a false sense of security regarding their children's online experience. Filters are unable to address all online risks, such as cyber-bullying, online sexual predators, viruses, or the theft of personal information.
- 9.3 The Department considers that the most effective way of ensuring that children have a safe online experience is through effective parental supervision.

10 Review of the Code

- 10.1 The Department, in conjunction with the IRG, will review the Code after 12 months operation.