INTERNET SERVICE PROVIDERS
SPAM CODE OF PRACTICE

A Code for Internet Service Providers providing Email Services

CO-REGULATION IN MATTERS RELATING TO SPAM EMAIL

(CONSISTENT WITH THE REQUIREMENTS OF THE UNSOLICITED ELECTRONIC MESSAGES ACT 2007)

August 2007
Version 1.00

InternetNZ
NZ Marketing Association
Telecommunications Carriers' Forum

EXPLANATORY STATEMENT

The ISP Spam Code of Practice (the Code) seeks to establish industry wide practices and procedures relating to Electronic Messages, as defined by the *Unsolicited Electronic Messages Act 2007* ("the Act"), that are Spam email.

Email is enormously beneficial to New Zealand businesses and End Users as a low cost and rapid communications medium. Access to email remains a primary reason for many New Zealanders going online.

Spam makes up over half the volume of email globally and imposes costs and inconvenience on End Users and Service Providers alike. As well as contravening the Act, Spam may also be offensive, or contain illegal or malicious codes and viruses.

There are five complementary elements in dealing with Spam:

- strong, effective domestic legislation;
- education of End Users;
- action by e-marketing and Service Provider industries;
- technological solutions; and
- international cooperative efforts.

In furthering these elements, industry including InternetNZ, the ISP Association of New Zealand (ISPANZ), the Telecommunications Carriers' Forum (TCF) and the Marketing Association (MA), along with like organisations, have been active in devising initiatives designed to combat the Spam problem by providing information to End Users, reviewing operational procedures and implementing "nospam" policies.

This Code recognises that action must be taken by Service Providers to help minimise Spam and its negative effects without unduly impeding legitimate business activities conducted over the Internet. Further, the Code has been drafted with regard to the MA's Code of Practice for Direct Marketing and the TCF's SMS Anti-Spam Code, which both deal with Spam related issues. Regard has also been paid to the TCF's Customer Complaints Code.

Regard has also been given to relevant RFCs (Requests for Comment) and to the RFC process in general. RFCs are the working notes of the Internet research and development community. These documents contain protocol and model descriptions, experimental results, and reviews. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs. New standards may be proposed and published on line, as an RFC. The Internet Engineering Task Force is a consensus-building body that facilitates discussion, and eventually a new standard may be established, but the reference number/name for the standard retains the acronym RFC, e.g. the official standard for email is RFC 2822. The Working Party is mindful of this being the appropriate medium for the development of new Internet standards.

Code Development and Review

The InternetNZ / TCF / MA Working Party ("Working Party") developing the Code has representation from a cross section of Service Providers and other interested parties. The development process for the Code is as follows:

(a) An initial draft Code is produced, which in the view of the Working Party achieves the objectives and will be acceptable to industry (the "Preliminary Draft").

(b) The Working Party will provide regulatory bodies including the Commerce Commission, the Department of Internal Affairs, the Ministry of Economic Development, and consumer bodies such as the New Zealand Consumers Institute and Telecommunications Users Association of New Zealand (TUANZ) with the Preliminary Draft for consideration and comment.

(c) The Working Party will consider and incorporate the recommendations from the reviewers of the Preliminary Draft as appropriate. The Working Party will provide reasons as to why any suggestions or comments have not been incorporated.

(d) The revised document (the Code) will then be released for an appropriate public consultation period.

(e) Further consultation will be undertaken by the Working Party as required and all submissions received by the Working Party during the public consultation period will be considered. The Working Party will document which recommendations have been incorporated and in respect of those (if any), which it is not able to incorporate, it will provide the reasons why they could not be accommodated. This record will form part of the Working Party's documentation when applying for acceptance to the Code from the following organisations:

(i) The Board of the TCF
(ii) The Council of InternetNZ
(iii) The Board of ISPANZ

Note: *The mechanism (statutory, regulatory or other) by which this Code can be considered to be adopted has yet to be determined. The comment above indicates InternetNZ's preliminary view that for the Code to have general effect, it will need to have been accepted and endorsed by the organisations listed above.*

Current Regulatory Arrangements

The Unsolicited Electronic Messages Act 2007 (“the Act”) came into effect on 5 September 2007. Under the Act it is illegal to send, or cause to be sent, ‘commercial electronic messages’ that have a New Zealand link and which are unsolicited. A message has a ‘New Zealand link’ if it either originates or was commissioned in New Zealand, or originates overseas but has been sent to an address accessed in New Zealand or a recipient present or carrying on business in New Zealand.

The Act covers Electronic Messages – including emails, mobile phone text messages (SMS), multimedia messaging (MMS) and instant messaging (IM) – of a commercial nature. However, the Act does not cover voice or fax telemarketing. The Act sets out penalties for the sending of unsolicited commercial Electronic Messages in breach of the Act. The Act also prohibits the use of address harvesting software or lists produced with such software in connection with the sending of unsolicited commercial Electronic Messages.

The Act addresses the Spam problem principally by targeting senders of Spam. However since senders of Spam require the services of Service Providers in order to send their Spam, enlisting the support of those Service Providers has the potential to be an efficient and also a more pro-active way of addressing the Spam problem. This illustrates the scope for the introduction of a co-regulatory Code on Spam for the Internet industry.

The Telecommunications Act 2001 does not impose any specific requirements on the industry in respect of Spam.

How the Code Builds on and Enhances the Current Regulatory Arrangements

The Code establishes minimum acceptable practices for Service Providers to follow in relation to:

(a) providing useful information to End Users on how to minimise Spam;

(b) dealing with Reports from End Users and Complaints from Customers regarding Spam;

(c) interacting with Law Enforcement Agencies on Spam-related matters within the context of the requirement to maintain the confidentiality of an End User’s personal information and when such personal information may be lawfully disclosed; and

(d) technical initiatives.

This is considered to be essential to the process of reducing Spam in New Zealand.

Benefits to Consumers

It is anticipated that adoption of this Code will benefit consumers by establishing practices to reduce Spam volumes and by the receipt of information on how to avoid and deal with Spam.

Benefits to Industry

It is anticipated that Service Providers will benefit from the adoption of this Code through reduced Spam volumes and therefore higher levels of Customer satisfaction and improved operational efficiency.

The Code rules, examples and explanatory comments have been written in plain English and framed in an easily understood manner to provide a certainty of understanding leading to consistency in their application throughout the industry by Service Providers.

Anticipated Cost to industry

Service Providers will incur some initial and ongoing costs in relation to compliance with this Code, depending on each Service Provider's current practices. Initial and ongoing costs can be expected in relation to the education and training of staff, development or enhancement of policies and procedures, development or modification of internal systems and employment of additional staff. Service Providers will also incur costs in reviewing their current privacy management practices, as certain of the obligations imposed by this Code will require such a review to ensure compliance with the Privacy Act 1993.

CONTENTS

PART A – PRELIMINARY

1. Introduction and Implementation

1.1 Introduction

1.1.1 This Code addresses the handling of certain Spam related matters by Service Providers and has been facilitated by InternetNZ, the Telecommunications Carriers' Forum (TCF) and the Marketing Association (MA) through the Working Party. The composition of the Working Party is representative of the New Zealand Telecommunications and Internet Industries. Importantly the Code development process has also involved input from other industry and non-industry stakeholders including Government regulators, agencies and consumer organisations. **Schedule 1** lists those industry and non industry players who have contributed to the development of this Code.

1.1.2 If there is a conflict between the requirements of this Code and any requirements imposed on Service Providers by statute, regulation or legally binding or code of practice (e.g., the Telecommunications Information Privacy Code 2003), the Service Provider will not be in breach of this Code by complying with the requirements of the statute, regulation or code of practice.

1.1.3 For the purposes of this Code, the acronyms, definitions and interpretations set out in clause 3 apply unless otherwise stated.

1.2 Ratification of the Code

This Code is to be submitted to the Council of InternetNZ and the Boards of the TCF and MA for acceptance.

1.3 Date of Implementation

This Code will come into effect from the date the Act comes into force, September 5, 2007.

2. Scope and Objectives

2.1 Scope

2.1.1 This Code applies to Service Providers as defined in the Act, where they are involved in the generaton, transmission or delivery of email.

2.1.2 This Code only applies to email that falls within the definition of an Electronic Message (as defined in the Act).

2.1.3 The requirements of this Code apply to Service Providers irrespective of the size of the organisation.

2.1.4 This Code excludes matters relating to e-marketing activities that are addressed in the Marketing Assocation Code of Practice.

2.1.5 Nothing in this Code limits the right of a user to remedies under other legislation such as the right to complain to the Privacy Commissioner under the Privacy Act, 1993.

2.2 Objectives

2.2.1 The objectives of this Code are to:

(a) provide rules and guidelines for Service Providers to promote the adoption of responsible processes and procedures for dealing with Spam;

(b) ensure these rules and guidelines are developed in such a way as to achieve a balance between legitimate industry interests and End User interests;

(c) reduce the volume of Spam being created within the Internet in New Zealand;

(d) reduce the volume of Spam being delivered to New Zealand email mailboxes;

(e) promote End User confidence in, and encourage the use of, the Internet; and

(f) provide a transparent mechanism for complaint handling by Service Providers in relation to Spam and any breaches of this Code, and ensuring that complaints are handled in a fair and efficient manner.

2.2.2 In seeking to achieve its objectives this Code applies the following principles:

(a) a fair balance should be maintained between legitimate industry interests and End User interests;

(b) any rules should not adversely affect the commercial viability of Service Providers and the services they make available; and

(c) Spam is an inherent risk when using the Internet and as such Service Providers and End Users each have responsibilities in attempting to minimise the Spam burden.

3. Terminology and Interpretation

3.1 Definitions

Acceptable Use Policy the published policy of a Service Provider governing the appropriate use amongst other things of email and the Service Provider’s network and services, and any terms and conditions upon which a Service Provider provides an email service, including where appropriate the grounds on which a Customer’s service can be terminated by the Service Provider.

Act the *Unsolicited Electronic Messages Act 2007*.

Botnet a group of Zombie computers under the control of one malicous third party.

Blacklist a list of web sites that are explicitly refused through a barrier such as a Spam Filter.

Code this code of practice.

Complaint "Customer Complaint" or "Complaint" means a genuine expression of dissatisfaction over a Spam issue.

A Complaint is:

* Customer initiated;

* about a specific Spam related event or events;

* a grievance that isn't resolved when it is raised or which the Customer has otherwise requested be recorded;

* valid under this Code if it is made within 28 days of the Customer's initial contact with the Service Provider in relation to the activity being complained about.

Content all forms of information and, without limitation, includes text, pictures, animation, video and sound recording, separately or combined and may include software.

Customer an End User with a contractual relationship with a Service Provider.

Electronic Message has the meaning given in section 5 of the Act.

End User any Person with access to an email account.

Enforcement Agency the Department of Internal Affairs, which is the authority responsible for administering the powers in Part 3 of the Act.

False Positive is a legitimate message incorrectly classified as Spam by a Spam Filter.

Home Page the primary page of the website of the Service Provider that is used to communicate to Customers and End Users, including to provide information regarding products or services of the Service Provider.

Internet Engineering Task Force the open network of individuals concerned with the evolution of the Internet architecture and the smooth operation of the Internet known as the "Internet Engineering Task Force" – creators of "RFC's". See www.ietf.org/rfc.html.

Internet (also known simply as the Net) is the worldwide, publicly accessible system of interconnected computer networks that transmit data by packet switching using the standard Internet Protocol (IP).

Internet Address the electronic address (domain name or IP address) of Content housed on the Internet. (c.f. Electronic Address in the Act)

Open Proxy a proxy server that would allow any user to relay Internet services such as e-mail and Web Pages, potentially for illegitimate purposes.

Open Relay an SMTP (e-mail) server configured in such a way that it allows anyone on the Internet to relay (i.e. send) e-mail through it.

Person includes individuals or organisations, as defined by the Act (subsection 4(1));

Report a notification to a Service Provider that Spam appears to have been sent through the Service Provider's network, or that there appears to have been a breach of the Service Provider's Acceptable Use Policy by a Customer of the Service Provider that is related to Spam.

RFC is a "Request for Comment", the accepted Internet standards documentation, as established by the Internet Engineering Task Force.

Sender Policy Framework a protocol used to mitigate e-mail forgeries. A line of Code called an SPF record is placed in a sender's Domain Name Server information, which can then be used by an incoming mail server to verify a sender before allowing a message through.

Service Provider has the meaning given to that term in section 4 of the Act and references to "Service Providers" are references collectively to Service Providers that have a legal presence in, or that are carrying on business in, New Zealand.

Spam an 'unsolicited commercial electronic message' as defined in section 4 of the Act.

Spam Filter any product or service that is designed to minimise, eliminate or quarantine suspected Spam.

Working Party the Anti-Spam Working Party as constituted from time to time. The current membership of the Working Party is set out in Schedule 1.

Web Page a file of Content that can be retrieved on the World Wide Web by accessing a single Internet Address.

Whitelist a list of web sites that are explicitly trusted and allowed through a barrier such as a Spam Filter.

Zombie a computer whose security has been compromised with a malicous third party having remote authoritative control over it.

3.2 Interpretation

In this Code, unless the contrary appears:

(a) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(b) words in the singular include the plural and vice versa;

(c) words referring to or implying persons include all natural and legal persons;

(d) a reference to a Person includes a reference to the Person's executors, administrators, successors, officers, employees, volunteers, agents and/or subcontractors (including but not limited to, persons taking by novation) and assigns; and

(e) where documents are referred to in this Code by means of Internet Addresses, the Internet Addresses are intended for reference only and the operation of the Code will not be affected where the document referred to is subsequently relocated to another Internet Address.

3.3 Abbreviations

APNIC: The Asia Pacific Network Information Centre

AUP: Acceptable Use Policy

DNS: Domain Name System

IETF: The Internet Engineering Task Force

InternetNZ: the trading name of the Internet Society of New Zealand (Inc)

ISPANZ: Internet Service Providers Association of New Zealand (Inc)

SMS/MMS: Short Message Service/Multimedia Message Service

SMTP: Simple Mail Transfer Protocol

SPF: Sender Policy Framework

TCF: Telecommunications Carriers' Forum

TCP: Transmission Control Protocol

WHOIS: a database query system that provides technical contact information and other details about a domain name registrant

CODE RULES

PART B – PROVISION OF INFORMATION

4. Provision of Information

4.1 A Service Provider will have taken 'reasonable steps' to provide information to Customers in respect to requirements of Clause 4.2, if they have provided all of the following and, together, the information provided under clause 4.1(a) and linked to under clause 4.1(b) address each of the matters required by clauses 4.2(a) to (g):

(a) information in an Acceptable Use Policy;

(b) a link from a reasonably prominent position on the Service Provider's website to an information resource covering Spam and Spam Filters;

(c) a link from a reasonably prominent position on the Service Provider's website to this Code;

(d) a statement to the effect that the Acceptable Use Policy defines Spam using the criteria set out in the Act;

(e) a statement to the effect that there are suspension and termination provisions in the Acceptable Use Policy which may be enforced at the Service Provider's discretion,

4.2 Subject to Clause 4.4, Service Providers must take reasonable steps to:

(a) inform Customers that everybody must comply with the Act and must not otherwise not engage in practices which would result in a breach of the Act;

(b) inform Customers of the existence of any Code of Practice applicable to Spam;

(c) inform Customers of any relevant changes or additions to legislation applicable to Spam;

(d) warn Customers of the consequences of breaching a Service Provider's Acceptable Use Policy in relation to the sending of Spam, including where applicable, the potential for termination/suspension of the Customer's account;

(e) advise Customers of:

(i) methods of minimising the receipt of Spam;

(ii) the availability of Spam Filters;

(iii) their right to make complaints to any ISP regarding Spam that appears to come from that ISP or their customers;

(iv) their right to make complaints to the Enforcement Agency about Spam and procedures by which such complaints can be made;

(v) their right to make complaints to other bodies about Spam where the Content is in some way contrary to law;

(f) inform Customers whether Electronic Messages addressed to them are subjected by the Service Provider to a Spam Filter by default, and provide a non-technical overview of the operations of that Spam Filter sufficient to assist customers in making informed choices; and

(g) warn Customers that the use of a Spam Filter may result in legitimate emails being falsly classified as Spam (False Positives).

4.3 In addition to steps outlined in 4.2 (a) – (g), Service Providers should also provide a link to an agreed industry or government web site on Spam.

4.4 Attached to this Code as Appendix A is a sample AUP fragment which sets out suggested clauses to deal with Spam related issues as required by this Code.

PART C – LAW ENFORCEMENT ISSUES

5. Law Enforcement Cooperation

5.1 Service Providers will comply with all lawful requirements of law enforcement and regulatory agencies in investigating Spam activity.

5.2 Service Providers must ensure that they make available to the Enforcement Agency (or its authorised nominee) contact details (valid during normal business hours) of the person/team within the Service Provider who is responsible for addressing Spam issues. This contact point will be used as the central interface point for all Spam related issues involving that Service Provider - including requests for investigation, provision of Spam related information to the Service Provider and requests for information or technical intervention (e.g. taking action to shut down high volume Spam on the Service Provider’s network).

5.3 Service Providers must ensure that they make available to the Enforcement Agency (or its authorised nominee) contact details (valid for all hours outside normal business hours) of the person/team within the Service Provider who can deal with urgent Spam related matters that must be addressed outside the process under clause 5.2. Such urgent out of hours action is expected to principally relate to requests to take action to, for example, shut down high volume Spam on a Service Provider’s network where such Spam adversely affects the Service Provider’s network, its customers and/or other parties.

5.4 For the purposes of clause 5.3 it will be acceptable for Service Providers to offer pager/call diversion arrangements in order to comply with the requirement for “24 by 7” contact availability. Reasonable contact/call back arrangements will be agreed with Service Providers consistent with their scale of operations and the probability of out of hours contact being required.

5.5 Service Providers shall participate in initiatives of, or in conjunction with, the Enforcement Agency in fighting Spam and/or share information with participants of those initiatives for the purpose of fighting Spam. The information that a Service Provider is required to share under this clause shall be limited solely to information identifying Spam sources and Spam messages, for example IP addresses of Spam sources and Spam message signatures, and shall not include contents of email messages.

PART D – SPAM FILTERS

6. Making Spam Filters Available

6.1 Spam Filters must be offered either directly to Customers or information must be provided in a reasonably prominent position on the Home Page of the Service Provider's website linking to the websites of third parties that provide a means for End Users to access or acquire Spam Filters.

6.2 Where relevant, Service Providers are entitled to charge a reasonable cost for Spam Filters offered in accordance with Clause 6.1, such reasonable cost to be determined having regard to the nature, scope and functionality of the Spam Filter involved. Service Providers must advise Customers of any costs associated with Spam Filters at the same time as offering the Spam Filter.

6.3 Where a Service Provider provides client side Spam Filters direct to Customers the Service Provider must take reasonable steps to ensure that the Customer is advised at the point of sale the methods by which the Spam Filter can be updated from time to time and further where information can be obtained regarding the continuing availability of the Spam Filter. Reasonable steps may include the sending of an email containing information or a link to the information on/from the webpage from which the Spam Filters are offered to Customers.

6.4 When offering Spam Filters to Customers pursuant to this Clause 6, Service Providers must not offer that filter in a way that would involve a contravention of the Commerce Act 1986 or the Fair Trading Act 1986.

6.5 The Code recommends that Service Providers use Spam Filters that comply with industry Best Practice as defined in Section 9 of this Code.

6.6 Service Providers must aim to minimise the risk of False Positives to the greatest possible extent. Service Providers should:

6.6.1 provide contact details to which End Users or others can report False Positive incidents relating to that Service Provider

6.6.2 consider the use of local Whitelists where whitelisted members are verified to comply with the Act

6.6.3 avoid the use of blacklists and other Spam classification services that are known to have False Positive rates significantly higher than the industry norm

PART E – SERVICE PROVIDER OBLIGATIONS

7. Open Relays, Open Proxies, Zombies and Botnets

7.1 Service Providers must restrict inbound connections to any service they manage that allows email forwarding on behalf of third parties. Such restrictions must limit access to the service to a closed user group relevant to the use of the application that the service facilitates.

7.2 Service Providers must require their Customers to adhere to the same restrictions as are required of Service Providers in clause 7.1.

7.3 Service Providers must provide, in their AUP, a clause that allows for immediate account disconnection or suspension when the Service Provider detects a Customer's computer is originating Spam, for example as an Open Relay, Open Proxy, Zombie, or as part of a Botnet. This clause should apply regardless of whether the Customer's system is being used to send Spam intentionally, through misconfiguration, or by other means not authorised by that third party including but not limited to through a Trojan horse or virus.

7.4 In the event of a Service Provider receiving notification of a Customer's system being responsible for the generation of Spam due to a breach of the Service Provider's AUP (which will contain the obligation to comply with the provisions of Clause 7.1), the Service Provider must take reasonable steps to notify the Customer of the breach. The Service Provider should provide reasonable assistance, if requested, to assist the Customer to comply with the AUP and the Service Provider should also set a deadline by which the Customer must demonstrate actions taken to comply with the AUP. However, in the case of a serious or continuing breach the Service Provider may exercise its powers of suspension or termination of the Customer's account as provided in the preceding clause.

7.5 Reasonable assistance in the preceding clause means the supply of information by the Service Provider in relation to the nature of Open Relays, Zombies and Botnets and suggested resolutions to the extent that the Service Provider can provide this.

7.5 Service Providers should retain in their AUPs the right to scan within the networks under their control, for Customers' misconfigured mail and proxy servers, and to suspend services to such Customers who fail to rectify such problems as are notified to them within a reasonable time period of receipt of such notice.

8. IP Address Information

8.1 Service Providers directly responsible for the assignment of IP addresses to their Customers must adopt a policy on retaining information pertaining to those assignments to allow a reasonable period to address complaints.

8.2 Experience in handling such complaints will inform Service Providers as to the optimal time for retention but as a minimum a default period of 90 days is recommended.

8.3 Service Provider policies should also ensure that the information retained is safeguarded and address such matters as security, authorised access for Spam complaints investigation, disclosure, retention for evidential purposes and destruction when no longer required. Staff should be trained in their responsibilities.

8.4 Service Providers are reminded of their general obligation to safeguard personal information under the Privacy Act 1993 and the Telecommunications Information Privacy Code 2003 issued by the Privacy Commissioner.

9. Best Practices

9.1 Service Providers are encouraged to consider and implement best-practice actions that can be taken to assist in the reduction of Spam while retaining an awareness of the risk of False Positives. Following are examples of practices and procedures that are currently being debated as best practice. These examples are not exhaustive or prescriptive as it is recognised that methods of generating and delivering Spam are constantly changing and therefore the best practices for dealing with Spam are also constantly changing.

Examples of Current Best Practice:

• A Service Provider will comply with all APNIC requirements in relation to the updating of WHOIS data including ensuring WHOIS data for any Service Provider’s customers is kept updated.

• Service Providers should impose reasonable limits on the rate at which outgoing email can be sent by their Customers using an Internet account of the Service Provider, as determined by the Service Provider as being appropriate for the usual requirements of Customers to that type of Internet account.

• Any server on an Service Provider's network that is used for the sending of email, including servers of the Service Provider's Customers, should have a reverse DNS entry.

• Service Providers should actively monitor the volume of inbound and outbound email traffic, to determine unusual network activity and the source of such activity, and should respond appropriately.

• Service Providers should allow their Customers to authenticate to their mail servers

using SMTP AUTH as specified in RFC 2554. Customers wishing to send email through the Service Provider's email server but who are not connecting through the Service Provider's network must be required to use SMTP AUTH or an equivalent mechanism to authenticate themselves.

• Where technically and commercially viable, operators of equipment (such as LNS or RAS hosts) which terminates user sessions with dynamically allocated addresses MUST cause such sessions' outgoing connections to be dropped where they are attempting to contact a remote host on TCP port 25.

• Service Providers should not distribute Customer Premises Equipment (CPE) for connection to the Internet by their Customers that is so configured by default as to be susceptible to unauthorised remote administration across the Internet.

• Service Providers should control automated registration of email accounts provided by the Service Provider so as to prevent accounts from being registered without direct human intervention by a Customer.

10. Setting an Example

ISPs will set an example to their customers by not sending Spam themselves.

PART F – REPORTING SPAM

11. General Requirements

11.1 Service Providers must advise End Users how to report Spam which is allegedly being sent by:

(a) one of the Service Provider's Customers; or

(b) another Service Provider's Customers.

11.2 In respect of clause 11.1(b), the Service Provider’s obligation is limited to notifying End Users that they should contact the other Service Provider (through the RFC 2635 convention 'abuse@' email address) or the Enforcement Agency, if they are receiving Spam which appears to be from a Customer of that Service Provider.

11.3 Service Providers must not impose any charges in respect of handling Reports from End Users.

11.4 Service Providers must maintain an 'abuse@' email address, in accordance with RFC2142, to allow End Users to make Reports.

11.5 Acknowledging Reports of Spam

11.5.1 (a) Service Providers may respond manually or use an auto-response to acknowledge Reports of Spam made to their 'abuse@' email address (or other email address as per 11.4 above).

(b) Regardless of whether an auto-response or a manual response is provided to the End User, the acknowledgement that the Report has been received must be issued to the End User within seven business days of receipt of the End User's Report.

11.5.2 The acknowledgement to End Users should include:

(a) information on how the Service Provider deals with Reports of Spam that relate to its Customers;

(b) information, or a link to information, informing the End User about options for reducing the volume of Spam;

(c) information, or a link to information, about how the End User can Report Spam to another Service Provider (see clause 11.2);

(d) information, or a link to information, about how the End User can bring a Spam Complaint to the attention of the Enforcement Agency;

(e) information, or a link to information, about the procedure by which an End User who is also a Customer of the Service Provider may escalate a Report about Spam into a Complaint; and

(f) information, or a link to information, about how the End User can complain about an Electronic Message that may be illegal under New Zealand law.

PART G – COMPLAINT HANDLING

12. Complaints from Customers about Spam

12.1 This section deals with the handling of Spam-related complaints to Service Providers by their Customers.

12.2 All Service Providers must have and follow a Complaint handling process which:

(a) has regard to any general industry codes on Complaint Handling;

(b) includes the timeframes in which the Service Provider aims to investigate the Complaint, provide a final response to the Customer and escalate the Complaint internally (as required);

(c) allows Customers to be represented by an advocate or authorised representative when making a Complaint;

(d) provides for the recording of Complaints, the Complaint details and the outcome of the Complaint;

(e) provides for a formal response to be provided to the Customer of the outcome of the investigation of a Complaint;

(f) provides for internal escalation of a Complaint at the Customer's request;

(g) advises the Customer of further avenues of recourse in the event that the Customer is not satisfied with the manner in which their Complaint has been handled, or the outcome of the Complaint including but not limited to the Customer’s ability to refer the matter to the Enforcement Agency; and

(h) subject to clause 12.4, does not impose any charges in respect of handling Complaints from Customers.

12.3 A Service Provider's publicly documented complaint handling process must:

(a) provide straightforward and easily understood information;

(b) provide contact details for the Customer to make a Complaint to the Service Provider;

(c) specify the form which such Complaints should take;

(d) list further avenues of recourse that are available if the Complaint remains unresolved;

(e) be provided to Customers upon request; and

(f) indicate the time frame in which the Service Provider will respond to complaints.

12.4 Complaint Handling Charges

A Service Provider must not impose any charges in respect of handling Complaints from Customers, unless the Service Provider can justify that the handling / investigative process for the Complaint is sufficiently onerous as to justify the levying of such a charge, and has discussed their intention to charge the Customer before handling / investigating their Complaint.

13. Complaints Regarding Breach of the Code by Service Providers

13.1 Complaints regarding a contravention of this Code by a Service Provider should be pursued through avenues such as the Telecommunications Disputes Resolution Scheme, the Disputes Tribunal, the Courts, or the Privacy Commissioner. It is anticipated that this Code be referenced as identifying best practice for ISPs in the handling of Spam email.

PART H - MISCELLANEOUS

14. Dates of Review

14.1 The full Code will be reviewed by the Working Party after one year from the date on which it came into effect.

14.2 The Working Party may decide to conduct an earlier review of the full Code or parts of the Code, if there is market-driven demand to do so. The review process will include consultation with Service Providers, consumer representative bodies and other relevant parties.

14.3 Any suggested amendments to the Code as a result of the reviews, will be submitted to the InternetNZ Council and to the Boards of the TCF and ISPANZ for approval.

SCHEDULE 1 – LIST OF CONTRIBUTORS

Anti-Spam Working Party

Jordan Carter (InternetNZ)
Laura Chamberlain (Vodafone)
Keith Davidson (InternetNZ)
Sylvia Devlin (The Marketing Association)
Alistair Dixon (TelstraClear)
David Farrar (InternetNZ)
David Harris (InternetNZ)
Anthony Hosking (Vodafone)
Simon Lyall (InternetNZ)
Keith Norris (The Marketing Association)
Brett Robertson (Telecom)
Steve Shearman (Touch Point)
Stephen Tyers (Jericho)
Jeff Mann (Jericho)
Zac Pullen (Property Ventures)
Robert Hunt (Plains Communications and ISPANZ)
Gael de Kerdanet (Calcium)
Richard Wood (InternetNZ)

The following organisations had the opportunity to comment on the Code prior to the Code being published for public comment:

Privacy Commissioner
Ministry of Economic Development
Commerce Commission
Consumers Institute
The Internet Safety Group (Netsafe)
BusinessNZ
Department of Internal Affairs

APPENDIX A – AUP Fragment

SUGGESTED EXCERPT FROM A SERVICE PROVIDER'S ACCEPTABLE USE POLICY IN RELATION TO SPAM

NOTE: This document provides an example for Service Providers only. It is permitted, and indeed encouraged, that the content and wording be adapted for the Service Provider's specific purposes. In this example, "we" refers to the Service Provider, "you" refers to the Service Provider's Customer, and "Service" refers to the service provided by the Service Provider to the Customer.

X. SPAM

X.1 Definition

In this section, "Spam" includes one or more unsolicited commercial Electronic Messages with a New Zealand link as defined in the Unsolicited Electronic Messages Act 2007, and derivations of the word "Spam" have corresponding meanings.

X.2 Acceptable use in relation to Spam

You may not use the Service to:

(a) send, allow to be sent, or assist in the sending of Spam;

(b) use or distribute any software designed to harvest email addresses in connection with the sending of unsolicited commercial Electronic Messages; or

(c) otherwise breach the Unsolicited Electronic Messages Act 2007 or any regulations made under the Act.

X.3 Our rights to suspend the Service

We may suspend our provision of the Service to you in the following events:

(a) if the Service provided to you is being used to host any device or service that allows email to be sent between third parties not under your authority and control; or

(b) if you are in breach of clause X.2 above;

provided however that we will first make reasonable attempts to contact you and give you the opportunity to address the problem within a reasonable time period. What is reasonable in this context will depend on the severity of the problems being caused by the open service or breach referred to above.

X.4 Customer to minimise risk of breach

You agree to use your reasonable best endeavours to secure any device or network within your control against being used in breach of clause X.2 above by third parties, including where appropriate:

(a) the installation and maintenance of antivirus and “malware” software;

(b) the installation and maintenance of firewall software; and

(c) the application of operating system and application software patches and updates.

Our right to suspend your account applies regardless of whether the open service is provided or the breach is committed intentionally, through misconfiguration, or by other means not authorised by you including but not limited to through a Trojan horse or virus.

X.5 Our right to scan for misconfigurations

We may scan any IP address ranges allocated to you for your use with the Service in order to detect the presence of open or otherwise misconfigured mail and proxy servers.

X.6 Our right to terminate the Service

If the Service is suspended and the grounds upon which it was suspended are not corrected by you within seven days, we may terminate the Service.