Network Acceptable Use Policy

LAST UPDATED: 23 November 2015

VERSION 1 which replaces:

- Network Acceptable Use Policy (for Schools) v2
- Acceptable Use Policy for Provider Managed Network Services v2

~~LAST UPDATED: 23 June 2015~~

~~VERSION 2.0~~

Comment [A1]:
We updated this policy, to combine similar policies previously applicable to schools and providers. This document shows changes made to the provider version.

Auckland Head Office
Suite 306, Geyser Building
100 Parnell Road
Auckland 1052
PO Box 37 118
Parnell, Auckland 1151

Wellington Office
Level 9, Bayleys Building
36 Brandon Street
Wellington 6011
PO Box 11 487
Wellington 6142

P 0800 LEARNING
P +64 9 972 1679
W www.n4l.co.nz
E info@n4l.co.nz

This policy applies to all ~~Providers~~customers using our managed network product and to ~~anyone using a Provider's Managed Network services.~~their users.

Contents

1 Introduction

We provide ~~Providers~~customers with ~~Managed Network services~~our managed network product in order to support educational outcomes ~~in schools.~~ While we won't normally intervene in a customer's use of our products, certain types of use are considered to be unacceptable, or can affect our ability to provide services to our other customers. For example, if a user on the network was to transmit spam, the ability of other users to send email could be adversely impacted.

This policy describes the uses of our ~~services~~ managed network product that we consider acceptable, and the approach we will take to remedying any unacceptable use. Breach of this policy by anyone using a customers managed network service is considered to be a breach of this policy by that customer as well as by that user, whether or not the customer had knowledge or gave consent for such use. It is therefore important that each customer understands and ensures compliance with this policy by its users.

We may amend this policy from time to time by posting a new version in the "Legal and Policies" section of our website.

Comment [A2]: These changes of name have been made throughout the document but, in order to highlight more substantive changes, they have only been marked here.

Comment [A3]: This policy only applies to our managed network product. We made this change throughout the document but, in order to highlight more substantive changes, only marked it up here.

2 Responsible Use

Users must use our managed network product in a responsible manner. This includes:

- not interfering with the availability of any services to others (whether those services are provided by us or anyone else);
- not otherwise negatively impacting on any networks, equipment or other parties; and
- using our managed network product in a manner consistent with ~~activities of a Provider in relation to~~ the delivery of educational outcomes.

3 Prohibited Use

3.1 ~~I~~Illegal Uses

Users must not use our managed network product in ways that may constitute a criminal or civil breach of any statute, regulations, government requirements or any other law of any country. This includes, without limitation, breach of intellectual property rights (such as copyright, trademarks, patents, trade secrets and confidential information); defamation; breach of obscenity laws and laws as to objectionable publications, such as pornography and hateful materials; fraud; theft; misappropriation of money, credit card details or personal information; breaches of privacy obligations; and breaches of trade practices legislation, examples of which are the Fair Trading and Consumer Guarantees Acts (New Zealand) and the Trade Practices Act (Australia).

3.2 Security and Protection of the Network

Users must not use our services to breach, to attempt to breach, or in ways that may breach, the security and operation of any network, equipment or any other system. This includes, without limitation, hacking, cracking into, monitoring, or using systems without authority; scanning ports (including scanning for open relays); improper configuration of mail servers and FTP servers enabling distribution of spam or unlicensed material by others; interference of service to any user or network (or activities that might encourage such interference by others) including mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks; denial of service attacks or activities which might encourage denial of service attacks by others; unnecessarily excessive traffic (including excessive pings); distributing viruses, or other harmful material or software; any communications across our network which do not accurately identify (or disclose in a manner that is misleading) addresses, headers, names and other relevant details; and using our network in any way as a staging ground for any of those breaches or to disable or "crack" other systems.

3.3 Harmful Material

Users may not use our network to transmit content that may be of a harmful or threatening nature. This includes, without limitation:

- threats of death or physical harm;
- sexually explicit or pornographic material;
- content that creates a risk of:
  - harm, loss, physical or mental injury, or emotional distress to anyone or any animal;
  - loss or damage to property; and/or
  - exploitation of children;
- content we deem to be hateful, violent, harmful, abusive, racially or ethnically offensive, defamatory, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), threatening, profane, or otherwise objectionable; and
- content we consider fraudulent, false, misleading, or deceptive.

3.4 Spam

Users may not use our services to transmit spam. Spam includes (but is not limited to) sending:

- unsolicited electronic messages without:
  - the recipient's actual or implied consent; and/or
  - an easy way for the recipient to stop receiving more such messages from the same source;
- messages that could reasonably be expected to provoke complaints;
- chain letters, pyramid schemes or hoaxes; and
- emails and messages that do not accurately identify the sender's return address, header or domain name.

4 Detecting Breaches

We monitor the flow of traffic across our network in order to optimise the performance of the network and to enable us to respond to any issues. We also receive network performance statistics from each ~~Provider's router~~our routers on your premises to ensure ~~its~~your connection is performing as expected. As part of these processes, activity that might indicate unacceptable use may come to our attention.

Users and customers must inform us of any breaches of this policy that come to their attention. Users should do so by ~~notifying the Provider, and each Provider~~contacting our customer (e.g. their school), and our customer should do so by contacting our helpdesk.

5 Breaches – What Will Happen

If a possible instance of unacceptable use comes to our attention, we will generally notify and/or work with the relevant ~~Provider~~organisation (s) to investigate the use and, if it is unacceptable, try to agree a suitable remedy. ~~Each Provider must implement any remedies as agreed~~ In the most serious cases, we may notify law enforcement agencies in accordance with~~, or directed by, us.~~ our Privacy Policy.

~~We~~If you are a provider of products or services to schools, we may also inform:

- schools ~~if the~~of your unacceptable use, if it has, or is likely to, impact ~~them~~the school, their ~~Users~~users, or their use of ~~Our Services~~our products; or
- ~~in some circumstances~~ the Ministry of Education~~.~~ of your unacceptable use, in some circumstances.

~~In the most serious cases, we may also notify law enforcement agencies of the unacceptable use in accordance with our Privacy Policy.~~

While any instance of unacceptable use is being investigated, we may disable the user's or the customer's access to any of our products. If we find a user has seriously breached this policy we may permanently revoke their or the customer's access to any of our services.

If the unacceptable use remains unremedied, then we may, without further notice, suspend, modify, restrict or terminate the customer's access to our services, either in part or in full.

Comment [A4]:
We made this apply consistently with our previous policy for schools.

Comment [A5]:
We clarified the wording, but to similar effect