Wireless Acceptable Use Policy

LAST UPDATED: 23 Nov 2015

VERSION 2

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 schools using a community wireless network in order to connect users to our managed network product. It applies in addition to the Network Acceptable Use Policy available at http://www.n4l.co.nz/legalandpolicies/.

1 Introduction

This policy describes the uses of community wireless networks that we consider acceptable with our products, and the approach we will take to remedying any unacceptable use. For the purposes of this policy, a community wireless network is a wireless network that extends access to our managed network product to beyond the school's boundary.

2 Use of Community Wireless

Schools may use our managed network product in conjunction with a community wireless deployment, but only in a manner consistent with activities of a school and in relation to the delivery of educational outcomes. Our managed network product cannot be used in conjunction with community wireless for any other purpose.

However we do not technically support wireless systems operated by schools. This is the sole responsibility of the school.

3 Community Wireless Requirements

The school is responsible for adhering to the following guidelines when using our network to provide community wireless access.

- Ensure the community wireless service can only be used by staff and students of the school concerned, using authentication that can identify the individual users concerned.
  - *Acceptable Authentication Examples:*
    - *IEEE 802.1x Port-based Network Access Control*
    - *Device control via MAC address*
    - *Installation of a digital certificate on the device*
  - *Unacceptable Authentication Examples:*
    - *Pre-Shared Keys*
    - *Open wireless*
- Keep filtering and firewalling configurations for community wireless access, the same as the configurations for general school use (in other words, filtering and firewalling policies must not be relaxed for community based access).
- Never use our network to provide or support a commercial wireless service (in other words, never resell, transfer, sub-license or otherwise commercially exploit or commercially make available to a third party all or any part of our managed network product) without first obtaining our written approval.

4 Detecting Breaches

We monitor the flow of traffic across our network in order to optimise performance and to enable rapid response to issues. We also receive network performance statistics from each school's router to ensure its connection is performing as expected. As part of these processes, activity that might indicate unacceptable use may come to our attention.

Users and schools must inform us of any breaches of this policy that come to their attention. Users should do so by contacting their school, and each school 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 work with the relevant school to investigate the use and, if it is unacceptable, agree a suitable remedy. Each school must implement any remedies as agreed with, or directed by, us.

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