MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Technology in Schools

Information and Communications Technology (ICT) Wireless LAN Infrastructure:

Policy and Standards for Schools

Version 1.0

July 2020

Document Information

Acknowledgements

The Ministry of Education, New Zealand, acknowledges with thanks the assistance and contribution of a number of organisations, institutions, statutory bodies, and individuals in the preparation of these Standards. In particular, the assistance of the following parties is acknowledged:

Torque IP, the Network for Learning, Nspire Technologies.

Table of Contents

A. FOREWORD 7
B. PURPOSE 8
C. DOCUMENT SPONSOR 8
D. OUTCOME STATEMENT 8
1. USING THIS DOCUMENT 9
1.1. Interpretation of this Document 9
1.1.1. Interpretation 9
1.1.2. Scope of this Document 9
1.1.3. Criteria for Use 10
1.2. Application of this document 10
1.2.1. Regulations, Codes and Standards 10
1.2.2. Regulatory Requirements and Codes of Practice - Wireless LAN 10
1.2.3. New Zealand and International Standards and Requirements 11
1.2.4. Variation from this Document 12
1.2.5. Conflicts 12
1.3. Definitions and abbreviations 13
2. REFERENCE DOCUMENTS 27
2.1. New Zealand and International Standards 27
2.2. Application of the Standards 28
3. GENERAL CONDITIONS 29
3.1. Wireless System Works 29
3.2. Wireless LAN Equipment 29
3.3. Minor Materials, Fittings and Consumables 29
3.4. Electrical Installation Works 29
3.5. Site Conditions 29
3.6. Passive optical lan equipment and design 30
4. WIRELESS SYSTEMS: DESIGN STANDARDS 31
4.1. General 31
4.2. Minimum Wireless Standards and Performance 32
4.3. Designing a wireless lan 32
4.3.1. Wireless LAN Interfaces 33
4.3.2. Network Requirements 33
4.3.3. Logical Network Design Considerations 33
4.3.4. Wireless Equipment Requirements 34
4.3.5. Determining Location of Wireless Access Points 34
4.3.6. IPv6 Compliance 37

4.3.7. Wireless Access Point – Physical Installation 37
4.4. Typical Wireless Requirements 38
4.4.1. Small Schools (1 – 250 Students) 39
4.4.2. Medium Schools (251-750 students) 40
4.4.3. Large Schools (751 to 3200 Students), Extra-Large Schools (>3200) 41
4.5. Wireless LAN System Selection 42
4.6. Allocation of WLAN System Equipment 42
4.6.1. General 42
4.6.2. Internal Wireless Access Points 42
4.6.3. External Wireless Access Points 42
4.6.4. Special User Cases for External Wireless Access Points 43
4.6.5. Wireless Backbone Connectivity Solutions 43
4.6.6. Point to Point External WAPs 43
4.6.7. Wireless Mesh 44
4.6.8. Retention of Existing Wireless Access Points 44
4.7. Wireless LAN Management and Security 45
4.7.1. Key Security Concepts 45
4.7.2. Device or User Authentication 45
4.7.3. MAC Address Filtering 46
4.7.4. Pre-shared Key or Password 46
4.7.5. Encryption Techniques 47
4.7.6. WPA2 Authentication 47
4.7.7. WPA3 Authentication 49
4.7.8. Captive Portal 49
4.7.9. Wireless LAN Management 50
5. WIRELESS LAN SYSTEMS: TECHNICAL REQUIREMENTS 52
5.1. General 52
5.2. Wireless acccess points 52
5.3. Wireless Controllers 52
6. WIRELESS LAN SYSTEMS INSTALLATION PRACTICES 53
6.1. General 53
6.2. Safety 53
6.3. Manufacturer’s recommendations 55
6.4. Documentation 55
7. WARRANTY AND SUPPORT 56
7.1. General 56
7.2. Manufacturer’s warranty 56

7.2.1. Hardware Warranty 56
7.2.2. Software Warranty 56
7.2.3. Service Level Agreements 56
8. QUALIFICATIONS 57
8.1. Installer qualifications and selection 57
8.2. Supplier qualifications 58
9. OTHER CONSIDERATIONS 58
9.1. Health and safety considerations 58
9.1.1. Hardware 58
9.1.2. Protection from Radiofrequency Electromagnetic Fields 58
9.1.3. Peripherals and Other Systems 59
10. APPENDIX 1: WIRELESS LAN REQUIREMENTS 60
10.1. Introduction 60
10.2. System overview 60
10.2.1. The Proposed System shall be: 60
10.2.2. The Proposed System WAP shall have at a minimum: 60
10.2.3. The Proposed System Controller shall have at a minimum: 60
10.2.4. How to read these requirements 61
10.2.5. Changes in this Standard - Transitioning to the new naming convention: 61
10.3. Warranty and Support 62
10.3.1. Hardware Warranty 62
10.3.2. Software Support - Firmware 62
10.3.3. Software Support - Management 62
10.4. Performance 63
10.4.1. Air Interference 63
10.4.2. Access Points (AP) Internal 63
10.4.3. Antenna 64
10.4.4. WLAN Roaming 64
10.4.5. Centralised Controller Solution 64
10.5. System Features 65
10.5.1. VLAN and Policy Support 65
10.5.2. Ethernet Support 65
10.5.3. Traffic Management 65
10.6. Security 66
10.6.1. Encryption 66
10.6.2. Authentication 66
10.6.3. Wireless Intrusion Protection, Detection (WIPO/WID) and Counter Measures 67

10.6.4. End Point Integrity Checking - Network Access Control....67
10.6.5. Guest Access and Control....67
10.7. Scalability....67
10.7.1. Expansion....67
10.7.2. IPv6 Support....68
10.8. Management....68
10.8.1. WLAN Management Software....68
10.8.2. Users and SSID....68

A. FOREWORD

The educational environment provides one of the most challenging frameworks for the operation of comprehensive structured information and communications technology (ICT) infrastructure solutions. It has exceptionally high requirements for reliability, fault-tolerance and service availability that exceed many other similar sized operating environments.

Educational providers are frequently at the leading edge of the technology and application lifecycle, with teaching systems often involving new and innovative applications, extensive use of graphical content, monitoring, and reviewing functions. They are also much more likely to involve the use of complementary technologies, including wireless and cabled monitoring systems, audio-visual applications, presentation applications, multi-media content, metering and control requirements and collaborative developments, than their commercial or government counterparts.

The modern school infrastructure shall address not only the standard applications of telephony and data connectivity, but shall also support the unique requirements of heavy burst-oriented network traffic requirements over relatively shorter periods associated with educational systems, extensive use of multi-media technologies, and both wired and wireless networking.

The goal of this document, *Ministry of Education: Technology in Schools Information and Communications Technology (ICT) Wireless LAN Policy and Standards for Schools v1.0* is to provide a reference document for cost effective design and construction of telecommunications distribution infrastructure for all facilities in New Zealand schools. It has been prepared to outline the minimum standards required to ensure consistency and compatibility of all new and existing Ministry of Education schools wireless LAN systems.

This document provides the technical standards which shall be followed for the design and technical performance of any ICT telecommunications infrastructure in facilities owned by Ministry of Education schools. It is updated regularly as Standards, school requirements and Ministry policy change. Prior to using this document the user shall confirm that they have the latest version. The latest version of this document may be obtained from:

https://www.education.govt.nz/school/property-and-transport/suppliers/technical-information/responsibilities-of-an-ict-contractor/.

B. PURPOSE

This document has been prepared by the Ministry of Education for use by New Zealand Schools and other organisations which participate in the design, supply and implementation of information technology infrastructure within New Zealand schools. The documentation addresses the planning for wireless LAN systems in new schools but applies equally to existing schools planning significant upgrades and extensions to existing infrastructures.

It provides guidance and minimum technical standards in the following areas:

a) Technical requirements for wireless LAN systems
b) Product selection and system dimensioning
c) Design, installation and testing environments
d) Wireless LAN administration and documentation

This document will assist in the provision of a robust high performance campus wide school wireless LAN infrastructure to enable full use of ultra-fast broadband and to maximise teaching and learning opportunities.

C. DOCUMENT SPONSOR

This document has been developed by and is controlled by the Ministry of Education. All queries, errors, omissions or suggestions are to be directed to the email address:- Hardware.Replacements@education.govt.nz, and/or:

THE GROUP MANAGER
BUSINESS SERVICES
EDUCATION INFRASTRUCTURE SERVICE
PO BOX 1666
WELLINGTON 6140

D. OUTCOME STATEMENT

By using this document, designers and installers will successfully meet the Ministry of Education's minimum standards for the design, installation and support of wireless LAN systems in operation within New Zealand schools.

1. USING THIS DOCUMENT

1.1. INTERPRETATION OF THIS DOCUMENT

1.1.1. Interpretation

For the purposes of this document, use the key words "*must*", "*must not*", "*required*", "*shall*", "*shall not*", "*should*", "*should not*", "*recommended*", "*not recommended*", "*may*", and "*optional*". These are to be interpreted as described in RFC2119.

RFC 2119 gives the following definitions:

1. ***"must" -*** This word, or the terms ***"required"*** or ***"shall"***, mean that the definition is an absolute requirement of the specification and mandatory.
2. ***"must not" -*** This phrase, or the phrase ***"shall not"***, mean that the definition is an absolute prohibition of the specification.
3. ***"should" -*** This word, or the adjective ***"recommended"***, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. ***"should not" -*** This phrase, or the phrase ***"not recommended"*** mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. ***"may" -*** This word, or the adjective ***"optional"***, mean that an item is truly optional. One vendor/ supplier may choose to include the item because a particular marketplace requires it or because the vendor/ supplier feels that it enhances the product while another vendor/ supplier may omit the same item. An implementation which does not include a particular option ***must*** be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option ***must*** be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

1.1.2. Scope of this Document

This document addresses the following areas:

a) Wireless LAN system and product selection for use in New Zealand schools.
b) Wireless LAN equipment installation in New Zealand schools.

1.1.3. Criteria for Use

All school ICT wireless LAN installation and upgrade work shall be in accordance with this document.

The Ministry requires that all schools, designers and installers of networks for schools shall use this document, in order to allow the school to fully participate in the e-learning environment and protect the investment in wireless LAN systems.

In addition to this document, the designer and installer shall refer to other sources for detailed design and installation guidance, such as relevant mandatory legislation, publications outlined in this document, and manufacturer installation guidelines.

1.2. APPLICATION OF THIS DOCUMENT

1.2.1. Regulations, Codes and Standards

All wireless LAN system works shall be carried out in accordance with the regulations, codes, and Standards listed within this document.

Where New Zealand and international Standards are referenced in this document the application of the Standard shall be, unless specifically stated elsewhere to the contrary, to the latest edition and amendments available on the date 30 calendar days prior to the issue of any request, quote, tender or proposal.

Where specifications or Standards, or any other references in this document refer in turn to other specifications, Standards or documents whether whole or in part, the strictest of those consequential references shall apply to this specification as if they were completely contained in the original reference.

1.2.2. Regulatory Requirements and Codes of Practice - Wireless LAN

There are two main regulatory requirements, these are covered by the Radio Communications Act and the Radio communications Regulation. Both of these documents can be accessed through the Radio Spectrum Management website through the following link:

https://www.rsm.govt.nz/about/our-legislation/

For the 5 GHz Wi-Fi devices, Radio Spectrum Management have released a document regarding prohibited channels and locations, this document can be found using the following link:

https://www.rsm.govt.nz/assets/Uploads/documents/b8c1468d8e/5-ghz-info-leaflet-2019-update.pdf

All Wi-Fi solutions shall select New Zealand as the location to ensure the 5 GHz prohibited channels are not used as they are reserved for GURL Aeronautical (Airborne Weather Radar).

Other than for compliance with the Electricity Safety Regulations 2010 and relevant New Zealand Codes of Practice, there are **no** other regulatory requirements for wireless LAN components or design practice in New Zealand. This includes electromagnetic compatibility.

1.2.3. New Zealand and International Standards and Requirements

The work covered by this document shall comply with relevant New Zealand and International Standards, Specifications and Technical Bulletins.

Various national and international standards are maintained by national standards bodies. New Zealand standards are generally developed is association with Australia, and are referred to as AS/NZ standards.

The Institute of Electrical and Electronics Engineers (IEEE) is an international body that, among many other things, creates and maintains the technical standards used in WLANs.

The Telecommunications Act 1987 gave Telecom New Zealand, now Spark New Zealand, along with any other Service Provider the right to refuse connection, or to disconnect from their networks, any equipment which does not comply with Permit to Connect specifications or equivalent. This Act has since been repealed and replaced with the Telecommunications (Residual Provisions) Act 1987. The current legislation that applies is the Telecommunications Act 2001, the Search and Surveillance Act 2012 and the Telecommunications (New Regulatory Framework) Amendment Act 2018.

For equipment connected to a service provider's network, compliance with Spark New Zealand's PTC Access Standards specification is a contractual requirement.

The Ministry of Education also have a number of ICT standards that shall be followed and the latest versions of these standards can be found at:

https://www.education.govt.nz/school/property-and-transport/suppliers/technical-information/responsibilities-of-an-ict-contractor/

The designers, installers and schools shall conform to all the requirements of this document.

1.2.4. Variation from this Document

Compliance to the requirements of this document may, under some circumstances, not be practical, or cost-effective, or an alternative solution may exist that better suits the conditions on site.

The designer, installer and school are advised, in the event that compliance to this document cannot be met, they shall obtain written approval for a variation before undertaking the non-compliant works from Hardware.Replacements@education.govt.nz and/or :

THE PROGRAMME MANAGER
TECHNOLOGY IN SCHOOLS
EDUCATION INFRASTRUCTURE SERVICE
PO BOX 1666
WELLINGTON 6140

1.2.5. Conflicts

If a conflict exists between the Standards or with the Scope of Works then the installer shall notify the Project Manager or their representative of any conflicts and seek clarification prior to continuation.

In general, the order of precedence shall be:

a) Statutory Codes and Regulations
b) The Ministry of Education publication *Technology in Schools, ICT Wireless LAN Infrastructure: Policy and Standards for Schools* (this document)
c) Standards and specifications within the tender or contract
d) Referenced New Zealand and international Standards

In situations where tender specific Standards, specifications, or both, exceed Ministry requirements, these shall take precedence.

1.3. DEFINITIONS AND ABBREVIATIONS

Term, Acronym, or Abbreviation	Definition
10/100 Mbps (or Mb/s)	100 megabits per second Ethernet. Can switch 'back' to the older 10 megabit standard.
10 GbE	10 Gigabit (per second) Ethernet
1 GbE	1 Gigabit (per second) Ethernet. When using copper cabling, can switch 'back' to the older 100 or 10 megabit standards.
802.11 protocols	A set of standards created by the Institute of Electrical and Electronics Engineers (IEEE). Each standard is created by a specially convened committee of the IEEE. Each committee is designated by a letter. The letter then becomes part of the standard name.
802.11 protocols – Allowable MIMO streams	Equipment that uses Multiple Input / Multiple Output technology transmits multiple radio signals at the same time. Each individual radio signal is transmitted by a unique radio and antenna. More streams provides increased data capacity. Note that the number of usable streams is equal to the lower of the number of streams supported by the AP or client.
802.11 protocols – Approximate indoor range	An indication, in metres, of the likely distance within which the AP will deliver reasonable performance indoors. There are numerous things that can interfere with the RF transmission, which weakens the signal. This effectively lowers the actual data rate. Outdoor range can vary tremendously, up to several kilometres, for most protocols. Actual distances achieved depend heavily on the type of antennae used, height of the AP, and geography of the region being covered.
802.11 protocols – Bandwidth	While the standard frequency provided is a 'reference', the actual frequency used varies around the reference. Bandwidth is a measurement in megahertz (MHz) of 'spread' of the actual RF transmission. A wider bandwidth allows faster data flow.
802.11 protocols – Frequency	This is a technical reference point, describing the mean radio frequency (RF) used to carry data, in Gigahertz. (GHz) Of particular note is that lower frequencies travel further, and are less susceptible to certain environmental considerations (such as wall construction). Higher frequencies provide more data capacity but do not travel as far as 2.4GHz.
802.11 protocols – Maximum data rate	The theoretical data transfer rate per stream, expressed in megabits per second (Mbit/s). A stream describes one logical connection between the AP and client device. The 802.11 specification and amendments specify transmission rates not actual throughput. Due to different access methods to the RF medium the typical throughput is half or less the data rate.
802.11 protocols – Release Date	The date each standard was confirmed by the IEEE. Note that standards tend to be implemented in 'draft' form before this date, and manufacturers release products based on the draft. Draft implementations might not work properly between different manufacturers or with standards compliant equipment once the standard has been confirmed.
802.11i	802.11i is a security amendment that has been ratified by the IEEE and is now part of the 802.11-2007 standard.

Term, Acronym, or Abbreviation	Definition
	802.11i mandates the use of strong authentication and authorization via 802.1X/EAP (Extensible Authentication Protocol) – Enterprise or Pre Shared Key – Soho (small office/home office) use. Enhanced Data Privacy is addressed with the use of a strong encryption method called Counter Mode with Cipher Block Chaining Method Authentication Code Protocol (CCMP) using Advanced Encryption Standard (AES). The Supplement also defines the optional use of Temporal Key Integrity Protocol (TKIP) using the RC4 cipher for older clients that do not support AES.
802.1X	IEEE 802.1X-2004 is a port based access control standard that allows or disallows traffic to pass through a port and therefore access network resources. When implemented with Wireless LAN the 802.1X authentication framework uses an Extensible Authentication Protocol (EAP) type with an authentication server to provide strong mutual authentication between the client and authentication server via the Wireless Infrastructure. In this mode, each user is assigned a unique key mechanism for access to the WLAN. This affords a high level of individual privacy. For WPA, TKIP encryption is used. For WPA2, AES encryption is used. AES is stronger than TKIP, thus providing additional network protection.
AAA **A**uthentication **A**uthorisation **A**ccounting	Common terms used to describe security infrastructure. These are three services commonly provided by a directory service. Authentication is the process of determining, with some agreed level of confidence, the current user of a wireless device. Often it is desirable to authenticate the user of the device. Alternatively, authentication can be applied to the device itself. Authorisation determines what the authenticated user or device is allowed to do on the network. For a small school, it might be sufficient simply to give each wireless device the same network access as a wired device. A school with a larger, or more complicated, network might provide different access depending on who the user is. Accounting is the tracking of network resource usage by end users to assist will capacity planning, billing etc. A school security solution will generally have some way to measure how much use is made of various services provided on the network.
AES	Advanced Encryption Standard AES is a strong block cipher used to encrypt 802.11 Wireless Data. AES uses CCMP and encrypts data in fixed blocks with the choice of 128, 192 and 256 bit keys. AES is a mandatory part of the 802.11i security standard and is stronger and more efficient than older TKIP based on RC4.
Air Time Fairness	Airtime fairness is a technique used to reduce the impact the slowest clients on a wireless network have in slowing down other users by reducing the number of opportunities the slow clients have to transmit data. On a wireless network, once a client (or AP) starts to transmit a wireless frame, all other wireless devices on the same channel

Term, Acronym, or Abbreviation	Definition
	shall wait until the transmission is finished before they can transmit. If a device is transmitting, the period of time that another device needs to wait before trying to transmit is determined by the size of the frame being transmitted and the transmit and receive data rates between the client and its AP. For example, a wireless frame transmitted to or from a client connected at a low data rate may utilize 10 milliseconds of airtime, whereas it may take only 100 microseconds for a client connected at a high data rate, so the high speed client could have sent 100 frames in the time the slow client takes to send one frame. Unfortunately this means that a single low speed client can slow down all of the other clients on the WLAN. The traffic to the lower speed client consumes much more airtime than the faster client and prevents the fast client from benefiting from its higher data rate. The 802.11 standards allow for all wireless devices within range and on the same channel to compete equally for an opportunity to transmit a data frame, so a fast client can spend most of its time sitting idly waiting for a slow client to finish transmitting a frame so they can have another chance to transmit. With airtime fairness, the 802.11 standard of equal opportunity for all clients is not used; rather the wireless system dynamically determines the exact amount of airtime each client is consuming in microseconds. It then adjusts the number of opportunities each client gets to transmit using algorithms that account for each client's characteristics, such as current throughput, distance from the AP etc. As a result slower clients get fewer opportunities to transmit than faster clients. This results in improved speeds for the faster client with little or no impact on the slower client. Note that airtime fairness does not form part of the 802.11 standards. Not all vendors support airtime fairness and those that do have different methods of deploying it.
Anywhere, any-time, computing.	An expression sometimes used to refer to the increased portability of computing devices and services.
Approved Wireless LAN Supplier	A Ministry approved WLAN supplier
Approved Wireless LAN Equipment	WLAN equipment supplied for installation in a school by an approved WLAN Supplier or via their agent or one of their channel partners.
Approved Wireless LAN Brands	WLAN equipment that has been deemed to meet the minimum Standards required by the Ministry and listed in the approved List of Switch brands and manufacturers
Band Steering	Some wireless vendors have developed band steering. This is the ability for an access point to offload a client from one radio to another based on the client's capabilities. E.g. an 802.11n capable client may be offloaded to a 5 GHz radio to ensure maximum performance for that client and to reduce the likelihood of the 2.4 GHz radio becoming overloaded.
Beamforming	Beamforming was first supported in the 802.11 standards in 802.11n and was refined in 802.11ac. It is a technique that focuses the power of the wireless signal sent out by a transmitting device in the direction of the receiving device. Beamforming improves both range and throughput. Typically 802.11 AP radios radiate the wireless signal from the antenna evenly in all directions (like the ripples in a pond when a

Term, Acronym, or Abbreviation	Definition
	stone is thrown in) so the signal coverage map is a circle. With beamforming, the radio has 2 or more antennae and by changing the phase difference between the signal being sent from each antenna it is possible to focus the radio power in the direction of the client (radio waves, like all other waves, from two or more different sources create interference patterns when they meet, and this can increase or decrease the amplitude of the resulting wave). This results in a coverage map that is not a circle, but instead has a lobe (or lobes). APs that support beamforming typically modify the antenna phase differences electronically each time the AP communicates with a new client – and also changes the phase differences dynamically as the client physically moves about during the communication session, so the coverage map for the AP can be continuously changing. Beamforming is either ***explicit*** or ***implicit***. Explicit beamforming is where the AP and client work together by sharing information on the radio channel characteristics to modify the radio signal for best performance, so both the AP and client shall have beamforming capability. Implicit beamforming is when only the AP has beamforming capability and it decides the best way to modify the signal based on dropped data packets. Explicit beamforming has the advantage of better performance but has the disadvantage that it will not work unless both the AP and client support the same version of beamforming. Implicit beamforming has the advantage that as long as the AP has beamforming capability it will work with any client, but has the disadvantage of not having the same level of performance as explicit beamforming. Beamforming was first supported in 802.11n which defined several optional methods for explicit beamforming. Explicit beamforming requires both the AP and client to support the same beamforming method and since the 802.11n standard had several optional methods, the market did not standardise on any method and so beamforming was not widely deployed (although some vendors did provide APs that had proprietary implicit beamforming). With 802.11ac implementing beamforming on devices is still optional for manufacturers, but if implemented a single beamforming method is prescribed so it is likely to become ubiquitous.
Bring Your Own Device (BYOD) (or Bring Your Own Technology BYOT etc.)	Often used to refer to an environment (e.g. school or workplace) that provides wireless network access of some sort (typically carefully secured internet) for people to use with privately owned devices such as laptops, netbooks, iPads, tablets and smartphones.
BSS	Basic Service Set Part of the 802.11 standard service set – the Basic Service Set refers to the communication between a single wireless access point and a wireless station.
Building backbone cabling	Cable that connects the building distributor to a floor distributor.

Term, Acronym, or Abbreviation	Definition
Building distributor	A device (typically a 10/100/1000 Mbps or 10 Gbps switch) that is the connection point to the campus backbone and connects (distributes) to all floor distributors
Campus	A facility with two or more buildings in a relatively small area e.g. a school.
Campus backbone cabling	Cable that connects the campus distributor to the building distributor(s).
Campus distributor	A device (typically a 1/10 Gbps Ethernet switch) that is the central point for a campus (or school) network. The campus distributor connects to the external telecommunications network and also interconnects all the campus buildings (via "campus backbone cabling" to each of the "building distributors")
Captive Web Portal	A Captive Web Portal is used to capture a user's HTTP request and redirect to a specific webserver for such purposes as Authentication, registration or Policy acceptance. CWP are largely used for hotspots and guest networks (e.g. in airport terminal lounges)
Category 5 (Cat 5)	A definition of cabling components that provides AS/NZS 11801.1 class D performance.
Category 5e	Any reference to category 5e shall be interpreted as category 5.
Category 6 (Cat 6)	A definition of cabling components that provides AS/NZS 11801.1 class E performance.
Category 6_{EA} (Cat 6_{EA})	A definition of cabling components that provides AS/NZS 11801.1 class EA performance.
CCMP	Counter Mode with Cipher Block Chaining Method Authentication Code Protocol (CCMP) is the default encryption method defined in 802.11i amendment. CCMP uses AES encryption and uses 128bit encryption in fixed length blocks. An 8 Byte Message Integrity Check (MIC) is used to ensure data integrity.
Channel	Each frequency range used by 802.11 wireless (2.4 GHz and 5 GHz) is split into channels each of which a subset of the frequency range. For example, the 2.4 GHz band (used in 802.11b, g, and optionally n) is divided into 14 channels. The frequency (mid-point) of each 2.4 GHz channel is 5 MHz away from the frequency of the next channel (with the exception of channel 14 which is 12 MHz away from channel 13). **2.4 GHz Channels** Not all 2.4 GHz channels are permitted to be used under local regulations in many countries. In most of the world (including NZ) channel 14 is not permitted, and in the US channels 12, 13 and 14 are not permitted. As a result, some wireless equipment from US vendors does not support channels 12, 13 and 14. For this reason it is strongly recommended that channels 12 and 13 are not used in schools as some user devices may have these channels disabled. Since the 802.11g and n protocols require a 20 MHz channel width, adjacent channels overlap and cause interference with

Term, Acronym, or Abbreviation	Definition
	each other. To overcome this, it is recommended that only channels 1, 6 and 11 be used as they do not overlap. **5 GHz Channels** In the 5 GHz frequency range there are far more channels specified in the IEEE standards, but again the allowable channels varies by country. The 5 GHz channels that are permitted in most countries are typically 20 MHz apart so there is no channel overlap using 802.11n in the lower speed 20 MHz mode, but if channel bonding is used for higher speed a 40 MHz channel is needed so there are issues with channel overlap. With 802.11ac the channel width required can be up to 160 MHz for the fastest data speeds, so channel overlap becomes a significant design consideration.
Channel Bonding	Channel bonding is a technique where adjacent contiguous 20 MHz wireless channels are combined into a wider channel to enable higher data rates. Channel bonding is typically only used in the 5 GHz range as there are insufficient non-overlapping channels available in the 2.4 GHz range. **802.11a,b and g Channel Bonding** 802.11a, b and g do not support channel bonding. **802.11n Channel Bonding** 802.11n supports bonding of two adjacent 20MHz channels to form a 40MHz channel. **802.11ac Channel Bonding** 802.11ac supports bonding of adjacent 20 MHz channels to form 40 MHz, 80 MHz and 160 MHz channels. The 160 MHz channels can be either two adjacent 40 MHz channels or an “80+80” configuration where two non-adjacent 80 MHz channels are bonded together.
Data Link Layer	The Data Link Layer is the 2nd layer of the OSI model. Its function is to provide reliable transit of data across a link between two devices. The data link layer groups the stream of bits of information being transmitted into units called “frames” (e.g. an Ethernet frame), adds checksums to the frames so the receiver can ensure the frame has been received without errors (if the checksum does not match it is discarded), provides an acknowledgement back to the sender that the frame was correctly (or incorrectly) received, and provides flow control to ensure a fast sender does not overwhelm a slow receiver. In most school networks the data link layer function will be performed by the network interface adapter (which also manages the physical layer).

Term, Acronym, or Abbreviation	Definition
Data Rate	Data rate is the rate that data is transmitted over a link and is measured in bits per second (bps) or bytes per second (Bps). A 1 Bps data rate is the same as an 8bps rate (1 Byte = 8 bits). The 802.11 standards determine maximum data rates (e.g. 802.11a has a maximum data rate of 54 Mbps). These maximum data rates are a theoretical maximum only and actual throughput in practice is significantly less due to network and security overheads, interference, distance, obstacles and user congestion. An AP with a single client and good real world conditions will typically have a throughput between half and two-thirds of the maximum data rate. With two clients trying to simultaneously transfer large files through the same AP, this throughput per client would typically be halved, and quartered for 4 clients. **802.11b Data Rate** The maximum data rate for 802.11b is 11 Mbps. **802.11a and g Data Rate** The maximum data rate for 802.11a or g is 54 Mbps on a 20 MHz channel. **802.11n Data Rate** The maximum data rate for 802.11n depends on the number of MIMO streams used (can be 1 – 4) and on the channel width used (can be 20 MHz or 40 MHz). For a 20 MHz stream the maximum data rate is 70 Mbps while for a 40 MHz stream it is 150 Mbps. So for 4 streams over a 40 MHz channel the maximum combined data rate is 600 Mbps. **802.11ac Data Rate** The maximum data rate for 802.11ac depends on the number of MIMO streams used (Wave 1 can have 1 - 4 streams and Wave 2 can have 1 - 8) and on the channel width used (Wave 1 can be 20 MHz, 40 MHz, or 80 MHz and Wave 2 includes 160 MHz). For a 20 MHz stream the maximum data rate is 96 Mbps, for a 40 MHz stream it is 200 Mbps, for an 80 MHz stream it is 433 Mbps and for a 160 MHz stream it is 867 Mbps. So the maximum combined data rate for a Wave 1 AP with 4 streams over an 80 MHz channel is 1.73 Gbps and the maximum combined data rate for a Wave 2 AP with 8 streams over a 160 MHz channel is 6.93 Gbps.
Device	In the context of this document, the term ‘device’ refers to any equipment that is part of a wireless or wired network. This can include a router, switch, PC, laptop computer, netbook, tablet, iPod, smartphone, PSP console, or any one of many other types of equipment.
Directory Service	A directory service is a network-based service that can maintain information about all network users and devices, and provides that information to devices on the network with appropriate security

Term, Acronym, or Abbreviation	Definition
	(see AAA). Directory services in common use are Microsoft's Active Directory (AD), Apple Open Directory, Novell eDirectory, various Linux options, or possibly an externally provided secure Identity and Access Management (IAM) service.
DSSS	Direct Sequence Spread Spectrum (DSSS) is a technique originally developed for military use to make wireless signals more secure and less susceptible to interference and jamming. The original signal is multiplied with pseudo random noise resulting in a scrambled signal that appears to be just noise. 802.11b uses DSSS.
EAP-TLS	EAP-TLS is an EAP (Extensible Authentication Protocol) method from Microsoft used in the 802.1X authentication framework. EAP-TLS requires a client side digital certificate. The digital certificate is used for identity validation instead of User Name or Password. Digital Certificates are considered a strong form of authentication as they can be marked as non-exportable and therefore difficult to forge.
EMC	EMC (electromagnetic compatibility) is the ability of electronic components and devices to work correctly when they are close together without being impacted by EMI. Typically it means limiting the electromagnetic disturbances from devices that generate EMI and having an adequate level of immunity in devices that are exposed to EMI
EMI	EMI (electromagnetic interference) is the electrical disturbances caused by rapidly changing electrical currents. High frequency EMI is often called RFI. Wireless networks are susceptible to high frequency EMI.
Enclosure	A housing for accommodation of equipment and cabling.
Encryption	The process of transforming data using an encryption cipher in order to render the data stream unreadable except with the key.
F/UTP	Foil/Unshielded Twisted Pair
Firmware	Firmware is defined as the internal operating system of the WLAN hardware
Floor distributor	A device (typically a 1Gbps switch) that is the connection point to the building backbone and connects (distributes) to data outlet ports in rooms
Frequency Ranges used by IEEE Wireless Standards	The frequency range is a key characteristic of a wireless standard, and is the mid-point of a range of radio frequencies used by that standard. The 2.4 GHz frequency range is used by 802.11b, g, and (optionally) n standards. The 5 GHz frequency range is used by 802.11n and ac.
Gbps	Gigabits per second
Horizontal cabling	Cable connecting the floor distributor to the telecommunications outlets (wall data ports).
ICT	Information and Communication Technology
IEEE	IEEE (Institute of Electrical and Electronics Engineers) is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of

Term, Acronym, or Abbreviation	Definition
	humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.
Independent advice	Independent advice is defined as advice from a suitably qualified person that has no vested interest or monetary gain to be obtained from the given advice.
IoT	Internet of Things – Typical use is sensors connected to the Wi-Fi network. These sensors could be used to monitor the teaching environment for CO_2, Noise, Lux (Light level), Temperature etc.
IP	Internet Protocol – A Layer 3 Protocol that allows the assignment of IP addresses to devices in a network for routing purposes.
IPv4	IPv4 is the most widely used version of the Internet Protocol. It defines IP addresses in a 32-bit format, which looks like 123.123.123.123. Each three-digit section can include a number from 0 to 255, which means the total number of IPv4 addresses available is 4,294,967,296 (256 x 256 x 256 x 256 or 2^32).
IPv6	IPv6, also called IPng (or IP Next Generation), is the next planned version of the IP address system. While IPv4 uses 32-bit addresses, IPv6 uses 128-bit addresses, which increases the number of possible addresses by an exponential amount. For example, IPv4 allows 4,294,967,296 addresses to be used (2^32). IPv6 allows for over 340,000,000,000,000,000,000,000,000,000,000,000,000 IP addresses.
Load Balancing	Often in a wireless network, many users will unknowingly be connected to the same AP, or even the same radio on the same AP, while neighbouring APs may be underutilised. This can have a significant impact on client performance and may cause users to have an unsatisfactory experience. It is logical, therefore, that clients be encouraged to move from the more heavily loaded APs to the lightly loaded ones. Some wireless vendors have developed load balancing to optimise the distribution of clients among access points.
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control, a hardware address that uniquely identifies each node of a network
Mbps	Megabits per second
Management Software	Management software is defined as the external application used to manage the configuration and administration of the LAN switching hardware.
Ministry (the)	Ministry of Education.
MIMO and MU-MIMO	MIMO (multiple-input and multiple-output) is a technique that uses multiple antennae and radios in wireless devices to exploit multipath propagation so that multiple wireless data streams can be sent/received simultaneously over a single channel. MIMO was first introduced in 802.11n. Both 802.11n and 802.11ac Wave 1 permit up to 4 simultaneous data streams over a single channel and they can only be used for a single client at a time.

Term, Acronym, or Abbreviation	Definition
	802.11ac Wave 2 devices will support up to 8 data streams over a single channel and the streams may be sent to multiple clients simultaneously – a technique called multi-user MIMO (MU-MIMO)
MOE	Ministry of Education
Network Cloud Controller	Cloud-based enterprise controller that makes it easy to build, manage and monitor your wired and wireless networks from anywhere in the world.
Network-Based Applications and Services	Applications include Student Management Systems, Learning Management Systems, financial systems, ePortfolio, email, etc. Services include file storage, printing etc.
NIC	A NIC (Network Interface Controller) is a computer hardware component that connects a computer to a data network. The most common network protocol supported by NICs today is Ethernet.
NMS	An NMS (Network Management System) is a combination of hardware and software used to monitor, report on and administer a network.
P2P	Point to Point
PCI	PCI (Peripheral Component Interconnect) is a local bus standard developed by Intel Corporation for attaching hardware devices (typically PCI cards) to a computer.
PEAP-TLS/MS-CHAP	Protected EAP is a Microsoft EAP method that uses TLS to provide an outer tunnel that is mutually validated prior to user credentials being submitted to the authentication server. PEAP-TLS uses a Digital Certificate for user identification; PEAP-MS-CHAP uses User Names and Passwords.
PKI	PKI (Public Key Infrastructure) is mechanism to enable users of a basically unsecure public network such as the Internet to securely and privately exchange data (and money) through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. PKI provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.
PoE	PoE (Power over Ethernet) is a network standard for sending DC power over data cabling to provide power for networked devices. The first PoE standard (IEEE 802.3af) provided up to 15 watts for a device. A new standard (IEEE 802.3at-2009) provides for up to 30 watts per device.
PPTP	The Point-to-Point Tunnelling Protocol (PPTP) is the most widely supported VPN method among Windows clients. PPTP is an extension of the Internet standard Point-to-Point protocol (PPP), the link layer protocol used to transmit IP packets over serial links. PPTP uses the same types of authentication as PPP (PAP, SPAP, CHAP, MS-CHAP v.1/v.2 and EAP).
PSK	PSK (Pre Shared Key) is a shared secret (passphrase or “key”) that has been shared using some secure method by two parties prior to the key being used. A PSK typically needs to be entered into a device in order to authenticate to an AP.
QoS	QoS (Quality of Service) is the ability to provide different priorities to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Term, Acronym, or Abbreviation	Definition
	QoS is important if the network becomes congested, especially for real-time streaming multimedia applications such as voice over IP, online games realtime video, since these are delay sensitive.
RADIUS	RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralised AAA management for devices to connect and use a network service.
RC4	RC4 is a streaming cipher used in SSL as well as 802.11 Wireless LAN WEP and TKIP.
RF	Radio frequency
RFI	RFI (Radio Frequency Interference) is high frequency EMI. Wireless networks are susceptible to RFI at certain frequencies.
RFP	Request For Proposal
Registered Jack 45 (RJ45)	In the United States of America, RJ45 is the Universal Service Ordering Code (USOC) for circuit configuration 45 (either T568A or T568B) for an 8-position modular connector. In this document RJ45 shall mean a modular 8-pin connector wired according to IEC 60603-7 configuration in accordance with AS/NZS 11801.1 Clause 10.6, figure 9, showing the jack layout and not specifically the required pair groupings (T568A and B) and pin assignments for IEC 60603-7 for Categories 5,6 and 6A Cabling.
Roaming	The ability for client devices to seamlessly transition from one AP and BSS to another (e.g. when moving from one location to another) while maintaining network connectivity for upper layer applications.
RSM	Radio Spectrum Management There are two main regulatory requirements, these are covered by the Radio communications Act and the Radio communications Regulation. Both of these documents can be accessed through the Radio Spectrum Management website through the following link; https://www.rsm.govt.nz/about/our-legislation/
SFP	Small Form-factor Pluggable (connector)
SNMP	Simple Network Management Protocol
SiDs	Safety in Design
SSID	SSID (Service Set Identifier) is a 32-character unique identifier for a WLAN. To communicate, all wireless devices (APs and end user devices) on a specific WLAN shall use the same SSID.
Structured Cabling System	A set of cabling and connectivity products that are constructed according to standardised rules to facilitate integration of voice, data, video, and other signals.
STP	Shielded Twisted Pair
Suitably trained person	A person that has completed and holds a certificate of competence for the equipment being installed, configured, monitored or maintained.
TCP/IP	Transmission Control Protocol/Internet Protocol are two protocols developed in the early days of the Internet by the U.S. military. TCP is associated with the assembling of data into packets and verifying delivery of the packets while IP is associated with the

Term, Acronym, or Abbreviation	Definition
	address part of each data packet so it gets to the correct destination. TCP/IP has become the foundation of the Internet. TCP/IP software is built into all major operating systems, such as Unix, Windows, and the Mac OS.
TDM	TDM (Time Division Multiplexing) is the process of combining multiple sources of data into one larger stream of data by allocating a time period to each source.
TKIP	TKIP (Temporal Key Integrity Protocol) is an enhancement to WEP encryption designed to address the weakness of WEP. TKIP mandates dynamic keys and Message Integrity Check (MIC) however it is still based on the RC4 cipher and offers lower performance.
TO	Telecommunications Outlet (typically a wall data port)
Traffic Separation	Network traffic from wireless devices can be combined with wired traffic, however, security can be improved by treating different types of traffic in a way that is appropriate for each type. Common criteria are the degree to which the device generating traffic is known and trusted, and any special requirements of that type of device. Traffic separation is usually implemented by the use of VLANs. Categories of traffic might include: a) Standard data traffic including staff b) Other school-owned devices c) Visitor wireless access d) Student wireless access (BYOD) e) Management of network devices f) VoIP Phone connections g) Streaming video, or video conferencing h) Security cameras
Unique Per User Pre Shared Key	Unique PSKs are unique WPA/2 PSKs created for each individual user/device on the same SSID. They offer the key uniqueness and policy flexibility that 802.1X provides with the simplicity of WPA/2-PSK.
UPS	Uninterruptible Power Supply
Uplink	A high-speed connection for aggregating traffic from an edge switch to a backbone switch or a server
UTP	Unshielded Twisted Pair
Virtual Server	Software that provides services on a network in the same way as a physical server. Multiple virtual servers can share the resources of one physical server.
Visitors/Guest	In this document, a visitor is anyone who might use a wireless network, but is not on the school staff, or regularly at the school. The implication is that these people will be welcome to use the school wireless Internet, but not other school network services such as file storage, or printing. Examples might be parents, students from other schools attending technology classes, Ministry of Education or ERO visitors, and contract workers.

Term, Acronym, or Abbreviation	Definition
	In a wider context, the term ‘guest’ is often used with a similar meaning when discussing wireless networks.
VLAN	A VLAN (Virtual Local Area Network) is a virtual network created within software on network switches. Multiple VLANs can share a single physical cable but are effectively separate networks. VLANs are typically used for traffic separation
VoIP	Voice over Internet Protocol
VPN	A VPN (Virtual Private Network) is secure (encrypted) private network created over any other (often unsecure) network.
WAP	Wireless Access Point
WEP	WEP (Wireless Equivalent Privacy) is a Layer 2 encryption method that uses the RC4 streaming cipher. The original 802.11 standard defined 64 and 128 bit keys. WEP should not be used, as it is relatively easy to “crack”.
Wi-Fi	Wi-Fi (Wireless Fidelity) is used generically to refer to any type of 802.11 network
Wi-Fi Alliance	A non-profit organisation that tests manufacturers’ 802.11 devices for compliance with the IEEE standards. Devices that pass testing are certified and are permitted to display the trademarked “Wi-Fi Certified” logo.
Wireless Bridging	Wireless bridges and routers are a point to point wireless deployment that allow access between buildings and campuses where wired Ethernet is not a cost effective option or a temporary connection is required. WLANs may be used to provide a cost effective alternative to extending the coverage of existing network infrastructures where reduced performance is acceptable.
Wireless Station	All components connected into wireless networks are referred to as wireless stations. All stations are equipped with a WNIC
WLAN	Wireless Local Area Network
WNIC	Wireless Network Interface Controller
WNMS	Wireless Network Management System
WPA2	WPA2 (Wi-Fi Protected Access 2) is a standards-based wireless security specification. It is often implemented with EAP for authentication and integrity checking and with TLS to provide encryption.
WPA2 Enterprise	Used to describe WPA2 implemented using a directory service, specifically a RADIUS server.
WPA2 Personal	The simpler way of implementing WPA2 is with a shared key, where each wireless device uses the same key. This essentially means the device is authenticated, rather than the user.
WPA3 Enterprise	WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocols across the network. WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data
WPA3 Personal	WPA3-Personal increased protection for individual users through provisioning of more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through

Term, Acronym, or Abbreviation	Definition
	Simultaneous Authentication of Equals (SAE), which replaces Pre-shared Key (PSK) in WPA2-Personal. The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

2. REFERENCE DOCUMENTS

Wireless LAN systems and equipment shall be installed in accordance with the manufacturer's specifications and Regulations, Codes and Standards listed below. Where New Zealand and international Standards are referenced in this document, the application of the Standard shall - unless specifically stated to the contrary - be in accordance with the latest edition and amendments available on the date 30 calendar days prior to the issue of any request for a quote, tender or proposal.

Where specifications or standards or any other references referred to in this document refer in turn to other specifications, standards or documents whether whole or in part, those consequential references shall apply to this specification as if they were completely contained in their entirety in the original reference.

2.1. NEW ZEALAND AND INTERNATIONAL STANDARDS

The work covered by this document shall comply with the following New Zealand and international Standards, Specifications and Technical Bulletins.

Standard/Specification or Technical Bulletin	Description
The Radio communications Act 1989	The Radio communications Act is our primary legislation. It sets out how we manage the radio spectrum in New Zealand.
The Radio communications Regulations 2001	New Zealand's Radio communications Regulations
The Telecommunications Act 2001	New Zealand's Act which deals with matters related to telecommunications services
Search and Surveillance Act 2012	This Act amends the Telecommunications Act 2001 (the **principal Act**)
Telecommunications (New Regulatory Framework) Amendment Act 2018	The purpose of this Act is to facilitate the monitoring of compliance with the law and the investigation and prosecution of offences in a manner that is consistent with human rights values
NZS 2772.1:1999	Maximum exposure levels – 3 kHz to 300 GHz (Radiofrequency Fields)
AS/NZS CISPR 22:2009	Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement
AS/NZS 1269	Occupational noise management
AS/NZS 2107:2000	Acoustics – Recommended design sound levels and reverberation times for building interiors
AS/NZS IEC 60825.2:2011	Laser safety – Safety of optical fibre communications systems
AS/NZS 3000:2018	Electrical installations (known as the Australian / New Zealand Wiring Rules)
AS/NZS 11801.1:2019	Information technology - Generic cabling for customer premises General requirements.
AS/NZS 3084:2003	Telecommunications Pathways and Spaces for Commercial Buildings

Standard/Specification or Technical Bulletin	Description
AS/NZS 3085.1:2004	Telecommunications Installations Administration of Communication Cabling System - Part 1: Basic Requirements
AS/NZS IEC 61935:2012	Balanced cable testing
AS/NZS 4117:1999	Surge protection devices for telecommunication applications
AS/CA S009:2019	Installation requirements for customer cabling (Wiring rules)
AS/NZS 61000.6.3:2012	Generic standards - Emission standard for residential, commercial and light-industrial environments This Standard is identical with and has been reproduced from CISPR/IEC 61000-6-3:1996
IEC-60297 **Part 1 and Part 2**	Dimensions of mechanical structures of the 482.6 mm (19 in) series
IEEE 802.3	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
ICT Cabling Infrastructure Policy and Standards for Schools v5.0	Ministry of Education Cabling Standards
Information and Communications Technology (ICT) Switching Infrastructure: Policy and Standards for Schools v5.00	Ministry of Education Switching LAN Standards
Electrical Infrastructure Policy and Standards for Schools v1.6	Ministry of Education Electrical Standards
AS 60118.4 -2007	Hearing aids
NZS 4121:2001	Design for Access and Mobility

2.2. APPLICATION OF THE STANDARDS

All school wireless LAN upgrade work undertaken throughout the Schools Network shall be in accordance with this Standard.

Wireless systems shall be designed and installed in accordance with this document by inclusion in tender and contract documents.

In the event of conflict between Ministry standards or specifications and other regulations, codes or standards the order of precedence shall be:

a) Statutory Codes and Regulations
b) Standards or Specifications within the tender or contract
c) The Ministry of Education publication *ICT Wireless LAN Infrastructure: Policy and Standards for Schools v1.0* (this document)
d) Referenced New Zealand and international Standards

3. GENERAL CONDITIONS

3.1. WIRELESS SYSTEM WORKS

The scope of work for the provision of wireless LAN systems and equipment in schools typically includes design, supply, installation, testing, commissioning, and documentation. Any new design shall include all 5 stages of Safety in Design (SiDs).

3.2. WIRELESS LAN EQUIPMENT

The wireless LAN system supplier/reseller shall maintain a list of equipment that complies with these Standards.

All equipment shall be new and selected to ensure satisfactory operation under the environmental conditions present at the site. The supplier/reseller shall comply with additional environmental conditions outlined in the Ministry of Education ICT Cabling Infrastructure Policy and Standards for Schools.

3.3. MINOR MATERIALS, FITTINGS AND CONSUMABLES

All materials, fittings or any work which is necessary for the installation and satisfactory function of the equipment or which is generally provided in accordance with accepted trade practices shall be provided or carried out as part of the works. Even though such material or work may not be explicitly mentioned in this specification or shown on the design drawings.

3.4. ELECTRICAL INSTALLATION WORKS

All electrical power system work shall be undertaken by qualified electricians in accordance with the relevant New Zealand Standards (AS/NZS 3000) and the Ministry of Education Electrical Infrastructure Policy and Standards for Schools.

3.5. SITE CONDITIONS

Suppliers shall undertake the necessary investigations to fully inform themselves of the site conditions which could impact the cost of the job. This shall include, but not be limited to, available cabinet space, environment conditions, and power provisioning. The installation of any wireless LAN equipment shall be deployed following the Ministry of Education ICT Cabling Infrastructure Policy and Standards for Schools e.g. Noise, Approved installers, Health and Safety, etc.

3.6. PASSIVE OPTICAL LAN EQUIPMENT AND DESIGN

This standard does not cover POL Equipment, however should a school, the Ministry or designer wish to deploy a POL solution within a school this shall be permitted providing it is signed off by a Ministry of Education representative. The POL cabling infrastructure shall be deployed following the Ministry of Education ICT Cabling Infrastructure Policy and Standards for Schools e.g. Product selection, Approved installers, Warranty etc.

Passive optical LAN ONTs shall provide the PoE required for WAPs to have full functionality. No more than two WAPs per PoE ONT shall be permitted and all ONT ports shall support a minimum of 1Gbps.

4. WIRELESS SYSTEMS: DESIGN STANDARDS

4.1. GENERAL

Because of the diversity of school sizes, building layouts, and wireless connectivity requirements, recommended wireless system configuration parameters are described. Schools are encouraged to discuss their requirements with an independent designer or consultant prior to purchasing hardware. The installation and configuration of any wireless system shall be completed by a suitably qualified person. Schools shall consider the following when implementing a WLAN system:

a) Require 1 Gbps PoE port on the Network LAN Switching in the cabinet to power new WAPs
b) Baseline configuration requirements
c) Present or future requirement of IP telephony on the WLAN
d) Guest Access
e) Requirement for management and reporting
f) Adherence to international and local Standards for connectivity
g) Ability to backup complex device configuration files and to restore to replacement devices in the event of a failure. Backups shall be taken after every configuration change
h) Total number of proposed wireless devices requiring connectivity (Tablets, Phones, iPod, Laptops, Chromebooks, printers etc.) on the WLAN, network segmentation and network use which may impact on other users
i) Complex security requirements such as segmenting administration and curriculum networks (protecting administration resources whilst allowing Internet access and messaging to all students and staff)
j) Requirements for bandwidth management; traffic prioritization, traffic shaping and traffic filtering
k) Requirement for future growth (e.g. IoT devices)
l) WLAN system shall meet at a minimum the technical parameters detailed in Appendix 1 of this document.
m) The ability of the management system to provide health checking, error and performance monitoring, and reporting
n) Ability of supplier to support product and respond to faults in a timely manner
o) Firmware shall be updated by the schools or its support provider every 6 months if an update is available.

10 Gbps Network switch connections or distribution shall only be implemented to support Wi-Fi 6 (802.11ax) if the majority of the traffic on the network is to an internal server, otherwise bandwidth to the internet shall be considered as the design bottleneck and therefore 10Gbps is not required.

Some of the above considerations can be particularly complex and will involve specialist product and wireless networking skills. Independent advice should be used to ensure that value for money is obtained when purchasing complex networking solutions. Independent advice is available from network.upgrades@education.govt.nz

4.2. MINIMUM WIRELESS STANDARDS AND PERFORMANCE

In order to maintain optimum wireless speed for client devices, Wi-Fi 5 (802.11ac Wave 2) with Wi-Fi Protected Access version 3 (WPA3) shall be the minimum standard for all new WAPs. The WAP shall also support Wi-Fi 4 (802.11n) and have dual radios supporting both 2.4 GHz and 5 GHz. All newly purchased WAPs shall be compliant with Mandatory parameters detailed in Appendix 1.

Devices using older wireless standards, such as 802.11g, can connect to Wi-Fi 4 (802.11n) compatible WAP, however when a slower device (which might be a device using an older standard, or be further from the WAP, or be behind a wall) is using the network, all other devices are forced to wait for it. This wait time is in the order of tens of milliseconds and, over time, it can cause a significant delay to other network users.

In a similar way, the 802.11n standard dictates that devices using WEP or WPA (not WPA2 or WPA3) encryption are only allowed to connect at 54 Mbps. Note that as well as having speed limitations, WEP and WPA are not recommended choices from a security perspective and shall be avoided if possible.

Handling of slow devices shall be addressed during the planning process for a school wireless network environment and implemented within the WLAN system configuration.

4.3. DESIGNING A WIRELESS LAN

School wireless networks have evolved from being predominately ad-hoc deployments in small areas through becoming part of school-wide infrastructure, to BYOD deployments where staff and students expect the network to always work, in all parts of the school campus. Early WLAN deployments focused on coverage. Over time, wireless standards and speeds have changed and there has been a mass increase in the availability of wireless capable client devices. WLAN deployments are now also about planning for client density, supporting the varied type of client devices (BYOD) and management of the WLAN for optimal performance and security.

The rapid widespread deployment of smart phones and tablets has placed significant demands on wireless networks in schools – particularly with uploading photos and videos to the cloud for storage, apps transferring data in the background, substantial use of social media, increased use of cloud based applications e.g. Google Docs, Office 365, proliferation of video in YouTube and access to other educational content and websites.

This section describes some of the technical considerations for wireless implementation and details the minimum mandatory requirements when implementing a WLAN within a school. Non-technical issues are described in School Wireless LAN Guidelines – Understanding Wireless

4.3.1. Wireless LAN Interfaces

Wireless LAN (WLAN) equipment conforming to the IEEE 802.11 standards is been being deployed as an access technology at the network edge in schools. Wireless bridges and routers are also available for access between buildings and campuses where wired Ethernet is not a cost effective option. WLAN may be used to provide a cost effective alternative to extending the coverage of existing network infrastructures where reduced performance is acceptable.

External point to point wireless bridges shall be protected against vandalism and misalignment (due to physical impact or vandalism) as much as is practically possible. Physical protection of an external WAP shall not be achieved through the use of metal cages as they may interfere with wireless signals.

Product selection shall now be based on Wi-Fi 4, Wi-Fi 5 and Wi-Fi 6 and the minimum for internal wireless access points shall be Wi-Fi 5.

4.3.2. Network Requirements

As wireless network technology has matured there has been a proliferation in manufacturer offerings of both equipment and management tools. At the same time there have been a number of architectural developments in the industry that are driving forward innovation as the industry moves to Wi-Fi 5 and beyond with Wi-Fi 6.

The initial planning for a wireless LAN is critical in determining criteria for choice of hardware and integrator. The product supplier shall be responsible for ensuring that the chosen solution fulfils the mandatory technical requirements in Appendix 1 and shall be a Ministry Approved Wireless Supplier and Brand.

School teaching and administrative requirements shall be articulated and recorded clearly before technical requirements are finalised.

4.3.3. Logical Network Design Considerations

A school WLAN designer shall consider the effect on the schools IP address range when deploying a wireless LAN (e.g. a BYOD policy will mean a significant number of new devices joining the network and requiring IP addresses). Failure to dimension sufficient IP address by the designer/ supplier/ installer shall be at their cost and not the schools. Any changes and costs associated with changing of IP addresses shall be provided to the school prior to commencing the installation of any new WLAN equipment.

While small schools may not need to invest heavily in detailed design, a medium, large or extra-large school shall undertake a detailed network design prior to implementing a WLAN solution due to the additional complexity that comes with increased device numbers. Designers shall refer to the “Technical Wireless Requirements” section of this document for the items that shall be considered and implemented based on schools size.

4.3.4. Wireless Equipment Requirements

Once the high-level plan is in place, Ministry approved WLAN equipment shall be selected for the infrastructure, based on the best fit to accomplish that plan.

4.3.5. Determining Location of Wireless Access Points

There are two methods for designing a WLAN solution, Predictive RF planning and Physical RF Mapping (Site Survey).

Predictive allows a designer to provide a school with costs to deploy a wireless solution to meet the specified requirements without a site visit, or for buildings that are not yet constructed. Schools shall always request that any plan includes, at a minimum, a predictive RF coverage map. This can then be tuned onsite with physical RF mapping, also referred to as a site survey.

A site survey is the process of measuring the RF coverage of a test WAP or the existing WLAN infrastructure. It can also be useful to measure other RF signals, both from wireless networks, and conflicting 'RF noise' from other devices, that might interfere with the school's new WAPs.

There are two aspects to a survey; each aspect contributes to the positioning of WAPs. Coverage determines the locations in a school campus where the wireless network shall be used, and Saturation describes the number of devices that the WLAN solution shall support in a particular location

Coverage shall be based on overlapping of 5 GHz channels in adjacent teaching spaces within the same building and Saturation shall be based on the number of concurrent devices the WLAN shall support as detailed in Appendix 1.

A wireless infrastructure scoping document shall be used to define the specific performance requirements for an installation. It shall include the proposed wireless applications, the total number and type of devices to be connected, the number of simultaneous connections required, and the bandwidth performance requirements broken down into areas of the school campus. This document is a critical part of the planning process. The network supplier shall be held to deliver to these requirements. Minimum requirements based on school size are detailed in "Typical Wireless Requirements" section of this document.

4.3.5.1. Coverage

There are two site survey coverage strategies that can be considered:

a) The most reliable approach is to perform a complete site survey before any deployment, to confirm the best locations for WAPs. Typically with this method, site survey professionals temporarily place WAPs in different locations, take measurements, and adjust their settings and locations as necessary. Once the optimum location for the WAPs has been determined, they will be permanently installed, and the system tested again to confirm installation quality. This method is the most reliable way to deploy a wireless network; however, it has increased costs and time. It also requires specialist hardware/software for taking the measurements.

b) An alternative strategy is to make initial estimates, with the help of a software planning tool, to determine the WAP locations, this is known as predictive mapping. The tool shall be configured with a school site map (floorplans etc.), indications of wall construction, and types of WAPs (Approved Brand) being considered. After the planning, the installers deploy WAPs according to the plan, then check to confirm that the network meets the requirements specified by the school. If there are coverage issues, additional WAPs can be deployed. If there is interference, or similar issues, the WAP locations can be adjusted.

The alternative strategy is usually less costly to implement. There should be few changes required for complete coverage. Any money saved though spending less time doing the survey can be invested in one or two more WAPs. Either strategy will result in the school getting a wireless network that meets the requirements they have specified. All newly deployed WAPs shall have a predictive RF plan created prior to deploying the solution and this shall be submitted with any cost estimates.

4.3.5.2. Capacity Planning

Sometimes there is a requirement for a very large number of user devices to connect wirelessly in one area. An example is a Hall, Gym or Library where dozens of students may be simultaneously using BYOD devices wirelessly.

Capacity planning, especially for high density areas, is a critical part of wireless implementation planning.

Typically most Wi-Fi 6 WAPs allow for two 1 Gbps switch ports either for resilience or for “link aggregation” to support the higher data rates of the WAP.

This shall be considered when allocating switch ports should a school implement a Wi-Fi 6 solution.

User Density on a wireless network

Many school wireless networks are no longer ad-hoc deployments in small areas. More commonly schools are adopting a BYOD policy which drives a staff and student expectation that the network shall always work, at acceptable performance levels, in all parts of the school campus.

Early WLAN deployments focused on coverage. Whilst coverage is still important what is also critical in delivering on these new expectations is planning for client density. With the proliferation of wireless capable devices including iPads, iPods, Smartphones, net books, laptops, chrome books and other tablet devices; it is possible that many users will have more than one device on hand and connected to the network simultaneously. A simple plan for coverage will not deliver on the expectation of the network always working or at acceptable performance levels.

Wireless networks, unlike wired networks, are a shared medium at the access level. A newly installed WAP shall provide the minimum specified amount of bandwidth, concurrent devices and concurrent multicast clients as specified in Appendix 1.

Catering for a high density of users can be more effective if the power of each WAP is lowered, as higher powered WAPs can interfere with each other’s radio signals.

This lowers coverage per WAP, so there may need to be more WAPs to compensate. Lowering the power of a WAP does not negatively affect saturation. The designer shall deploy the number of WAPs to provide the required device density based on each WAP supporting a minimum of 150 concurrent devices and 60 Concurrent multi-cast streams.

Most wireless technologies provide a variety of techniques to ensure that adequate capacity is available to the users. The following mandatory and highly desirable WLAN parameters shall be available in any newly installed WLAN system;

a. Quality of Service (Mandatory)

b. Load Balancing (Mandatory)

c. Band Steering to make maximum use of the available 2.4 Ghz and 5 GHz radios. (Mandatory)

d. AirTime Fairness (Highly Desirable)

It is critical to consider and plan for any expected high density wireless use areas in a school campus.

4.3.5.3. Roaming

Any device connecting to a school WLAN shall be able to move seamlessly from one WAP to another within coverage, using network services without the need for re-authentication. This is known as seamless roaming. This is especially important when authentication is provided by 802.1X. The selected WLAN infrastructure shall support Fast Roaming with key caching and Layer 3 mobility to facilitate inter-subnet roaming. This allows users to move about freely and remain connected to the network without their applications/services dropping out. Refer to Appendix 1 for mandatory WLAN System roaming parameters.

During the design phase the network shall provide overlapping coverage in areas where seamless roaming is required and this shall be validated during the post implementation survey phase. If a service is 'broken' by moving around in this way, the integrators shall diagnose why, and rectify any problems within the wireless network at no additional cost above the original implementation scope of works.

4.3.5.4. Power over Ethernet (PoE)

Enterprise class WAPs support Power over Ethernet (PoE). PoE is a mechanism for sending power over standard Ethernet cabling to run remote devices, such as wireless APs, VoIP phones and CCTV cameras

The relevant IEEE PoE standards are 802.3af, which provides a maximum of 15W of power per port and 802.3at which provides a maximum of 30W per port.

PoE allows for flexibility in WLAN deployment as it means WAPs do not require power outlets, and can be easily moved to meet requirements. All newly installed WAPs shall be powered by a PoE Switch LAN port as per the Ministry of Education - Information and Communications Technology (ICT) Switching Infrastructure: Policy and Standards for Schools.

With Wi-Fi 5 and Wi-Fi 6, the power requirements of WAPs has increased and 802.3af switches or injectors are unlikely to have sufficient power, therefore 802.3at compliant switches are required. The supplier of the WLAN system shall provide the power requirements for full functionality of a WAP. Some brands of Wi-Fi 5 and Wi-Fi 6 WAPs will operate on 802.3af but reduce the number of radio chains in use (typically on the 2.4 GHz radio) e.g. reduce the a 2x2 2.4 GHz radio down to 1x1 2.4 GHz radio so that it can operate.

PoE capable switches are more expensive than non-PoE capable switches, consume more power and generate more heat. They may also need fans for cooling and can be noisy, so mounting location and noise compliance shall be as per the *Ministry of Education - Information and Communications Technology (ICT) Cabling Infrastructure: Policy and Standards for Schools*.

4.3.6. IPv6 Compliance

The current version of the Internet Protocol (IP) being used in almost all school networks is known as version 4, or IPv4. A new version of IP, IPv6, is being increasingly deployed, and is likely to be a very important upgrade option for schools over the typical lifetime of a WAP.

All WLAN equipment installed within school network shall meet the minimum IPv6 requirements detailed in Appendix 1. Suppliers shall verify that their equipment meets all the mandatory requirements of this standard and supply records of IPv6 compliance testing. This information will give the school confidence that equipment will be able to use IPv6 as it becomes common.

4.3.7. Wireless Access Point – Physical Installation

The Wireless Access Point (WAP) mounting methodology is critical to ensuring the coverage, performance, connection reliability and aesthetics' are maintained. Therefore, in order to maintain installation quality throughout, the nominated contractor shall be responsible for the mounting of access points in locations identified by a wireless plan and to the manufacturer's mounting instructions.

All internal WAPs shall have the ability to be mounted vertically on walls, horizontally on "L" brackets, fixed ceilings and on ceilings grids. All external WAPs shall have the ability to be mounted vertically or horizontally. The supplier shall ensure that any brackets required are included along with mounting instructions for each mounting orientation detailed on the design.

It is expected that the majority of schools will not have high level T/Os (Telecommunications Outlets - Data Outlets) for patching WAPs, and these will be patched from local outlets at ground level (with appropriate trunking). All WAP mounting and trunking installation shall be included within the scope of works of a Ministry Approved ICT Cabling Contractor.

WAPs mounted in locations that may be exposed to potential physical damage, shall be protected by a high impact non-metallic enclosure or cage.

The following locations shall have physical protection installed for WAPs;

a) Gyms
b) Multipurpose Halls
c) Accessible external locations or where expose to potential physical impact from flying objects e.g. Balls

The nominated installer shall be responsible for the tidy installation of PoE switches and patch leads required to power and connect WAPs to the network.

If the installation is the replacement of an existing solution, then once the new system is cut over and operational, the contractor shall undertake physical removal (demounting and disconnection from the network) of all old WAPs.

4.4. TYPICAL WIRELESS REQUIREMENTS

With a number of schools implementing BYOD or allowing guest/ visitor access to their wireless network it is important to use traffic separation. This technique can improve network security and performance. As a general rule, a school campus with greater than 250 connected network devices in the present, or near future, shall give consideration to implementing network traffic segmentation through the use of VLANs.

Traffic separation is best accomplished by including the use of Virtual Local Area Networks (VLANs). As the name suggests, a VLAN is a virtual network and it is created within software on network switches. A VLAN shares most characteristics of a physical Local Area Network (LAN), except that multiple VLANs can share a single physical cable. A network can be deployed so a user can select between multiple networks available from each WAP (each different wireless network would have a different SSID). The network they choose (via the SSID) determines which VLAN they go in to. Each VLAN can have a unique set of characteristics (such as services available, network speed and priority, monitoring etc.) applied to network activity.

The planning and configuration of VLANs and SSIDs needs to be considered carefully by a network architect. Details are beyond the scope of this document.

The recommended maximum number of SSIDs deployed on a network shall be three, this is to limit the amount of beaconing or overhead on the WLAN system.

4.4.1. Small Schools (1 – 250 Students)

For small schools wireless network performance and management becomes an issue as schools may have limited access to resources and local expertise, and therefore the wireless deployment and architecture should be simplified where possible, without compromising security. The follow should be considered when designing a small school's wireless network;

a) Wireless Coverage (internal and external)
b) Bandwidth on links between switches
c) Internet connection performance
d) Latency for voice, video and other real time applications
e) IP addresses (Ensure sufficient expansion of the DHCP scope is provided, especially if BYOD or IoT devices are being implemented)
f) Number of devices requiring connectivity within a space
g) Video based, Apple TV and Chromecast type devices
h) Wi-Fi CCTV devices (Recommend these be avoided as they will place unnecessary load on the school WLAN network).
i) Cloud services e.g. Google Docs, Microsoft O365 etc.

Optimising the WLAN, the following configuration requirements shall be implemented:

i. Select New Zealand as the region within the WLAN System
ii. 2.4 GHz – turn on channels 1 to 11, do not turn on channels 12 or 13
iii. 5 GHz – turn on all channels (including DFS), Exclude prohibited Channels at locations detailed by RSM.
iv. Enable background scanning for Auto Channel selection configuration; minimum frequency should be every 40 seconds
v. Fix channel width to 20 MHz for 2.4 GHz frequency (not Auto)
vi. Fix channel width to 40 MHz for 5 Ghz frequency (Shall be detailed on commissioning/handover report, do not assume it is on or off by default)
vii. Band Steering – Set 2.4 GHz to 25% of total Clients
viii. Minimum throughput set to 5.5 Mbps
ix. Direct all guest traffic to the internet only
x. All newly installed WAPs shall be directly connected to an appropriately powered level of PoE port on a switch.
xi. The WLAN system shall be designed to provide 2.4 GHz overlapping coverage when teaching spaces are directly adjacent to each other (e.g. same building).

4.4.2. Medium Schools (251-750 students)

For medium schools wireless network performance becomes an issue as users compete for limited network resources such as:

a) File server processor and data transfer performance (If applicable)
b) Bandwidth on links between switches
c) Bandwidth on links to file servers (If applicable)
d) Connectivity to onsite Student Management System (Recommend cabled connection)
e) Internet connection performance
f) Latency for voice, video and other real time applications
g) IP addresses (Ensure sufficient expansion of the DHCP scope is provided, especially if BYOD or IoT devices are being implemented)
h) Number of devices requiring connectivity within a space
i) Wireless Coverage (internal and external)
j) Video based, Apple TV and Chromecast type devices
k) Wi-Fi CCTV devices (These shall be avoided).
l) Cloud services e.g. Google Docs, Microsoft O365 etc.

Optimising the WLAN, the following configuration requirements shall be implemented:

i. Select New Zealand as the region within the WLAN System
ii. 2.4 GHz – turn on channels 1 to 11, do not turn on channels 12 or 13
iii. 5 GHz – turn on all channels (including DFS), Exclude prohibited Channels at locations detailed by RSM.
iv. Enable background scanning for Auto Channel selection configuration; minimum frequency should be every 40 seconds
v. Fix channel width to 20 Mhz for 2.4 GHz frequency (not Auto)
vi. Fix channel width to 40 Mhz for 5 GHz frequency (Shall be detailed on commissioning/handover report, do not assume it is on or off by default)
vii. Band Steering – Set 2.4 GHz to 25% of total Clients
viii. Minimum throughput set to 5.5 Mbps
ix. Create separate VLANs on the switching network for Staff, Students and Guests (Refer to the Ministry of Education Information and Communications Technology (ICT) Switching Infrastructure: Policy and Standards for Schools)
x. Direct all guest traffic to the internet only
xi. All newly installed WAPs shall be directly connected to an appropriately powered level of PoE port on a switch
xii. All newly installed WAPs shall be directly connected to a PoE port on a switch.
xiii. The WLAN system shall be designed to provide 5 GHz overlapping coverage when teaching spaces are directly adjacent to each other (e.g. same building).

4.4.3. Large Schools (751 to 3200 Students), Extra-Large Schools (>3200)

A typical large or extra-large school network connects multiple buildings across a high-performance switched backbone and may have requirements for high availability and manageability. This is an important consideration in handling high-bandwidth or time dependant applications and services such as IP telephony, video conferencing and IP multicast applications when deploying a WLAN system.
Large and extra-large school network design shall include allowance for;

a) File server processor and data transfer performance (If applicable)
b) Bandwidth on links between switches
c) Bandwidth on links to file servers (If applicable)
d) Connectivity to onsite Student Management System (Recommend cabled connection)
e) Internet connection performance
f) Latency for voice, video and other real time applications
g) IP addresses (Ensure sufficient expansion of the DHCP scope is provided, especially if BYOD or IoT devices are being implemented)
h) Number of devices requiring connectivity within a space
i) Wireless Coverage (Internal and external)
j) Video based, Apple TV and Chromecast type devices
k) Wi-Fi CCTV devices (These shall be avoided).
l) Cloud services e.g. Google Docs, Microsoft O365 etc.

Optimising the WLAN, the following configuration requirements shall be implemented:

i. Select New Zealand as the region within the WLAN System
ii. 2.4 GHz – turn on channels 1 to 11, do not turn on channels 12 or 13
iii. 5 GHz – turn on all channels (including DFS), Exclude prohibited Channels at locations detailed by RSM.
iv. Enable background scanning for Auto Channel selection configuration; minimum frequency should be every 40 seconds
v. Fix channel width to 20 MHz for 2.4 GHz frequency (not Auto)
vi. Fix channel width to 40 Mhz for 5 GHz frequency (Shall be detailed on commissioning/handover report, do not assume it is on or off by default)
vii. Band Steering – Set 2.4 GHz to 25% of total Clients
viii. Minimum throughput set to 5.5 Mbps
ix. Create separate VLANs on the switching network for Staff, Students and Guests (Refer to the Ministry of Education Information and Communications Technology (ICT) Switching Infrastructure: Policy and Standards for Schools)
x. Direct all guest traffic to the internet only
xi. All newly installed WAPs shall be directly connected to an appropriately powered level of PoE port on a switch
xii. The WLAN system shall be designed to provide 5 GHz overlapping coverage when teaching spaces are directly adjacent to each other (e.g. same building)

4.5. WIRELESS LAN SYSTEM SELECTION

The Ministry may from time to time hold tenders for Approved WLAN Suppliers (Vendors) to provide equipment specifically for use in school ICT environments.

Schools that purchase WLAN equipment to install on their networks shall ensure the devices selected and the WLAN system architecture implemented comply at a minimum with this Standard and the mandatory parameters detailed in Appendix 1.

To facilitate ease of supplier product selection, an Approved WLAN Supplier list can be obtained from the Ministry of Education website, products from this list shall be used in the first instance and permission to deviate from the approved WLAN Brands shall be obtained in writing from a Ministry of Education EIS representative.

4.6. ALLOCATION OF WLAN SYSTEM EQUIPMENT

4.6.1. General

The Ministry, through a centralised tender process have created a panel of approved WLAN Suppliers to provide schools with access to WLAN equipment that complies with the warranty, support and replacement requirements which will meet and exceed the technology, design and implementation Standards as set out in this document.

4.6.2. Internal Wireless Access Points

All internal WAPs shall support the following minimum requirements

a) Wi-Fi 5 (5 GHz), Wi-Fi 4 (2.4 GHz)
b) Two radios, one 2.4 GHz and one 5 GHz
c) 4x4:4 5 GHz MU-MIMO and 2x2:2 2.4 GHz MU-MIMO
d) Load balancing between WAPs
e) 8 SSIDs
f) Beam forming
g) Antenna signal gain
h) Auto-channel selection
i) Omni-directional antennae
j) Band steering (between 2.4 GHz and 5 GHz)
k) Support Wall (vertical), Ceiling and Ceiling grid mounting
l) Support 150 concurrent devices

4.6.3. External Wireless Access Points

External WAPs shall provide external coverage of areas adjacent to a teaching space or outside areas for which a school wishes to use mobile wireless devices. The area of required coverage shall be defined and signed off by the school and a suitable solution using the same Brand as the internal WAPs shall be installed to ensure continuity of management and connectivity. There are also additional special use cases for implementing external WAPs.

4.6.4. Special User Cases for External Wireless Access Points

The issue of extending coverage to remotely located, moveable/portable buildings and special usage or temporary buildings is where external WAP deployments shall be considered.

Although each school site is unique, the following situations are suitable for considering connectivity using external WAPs:

a) Remote buildings
b) Special usage buildings (e.g. Caretakers shed, Board of Trustees owned)
c) Temporary buildings
d) Mobile/moveable buildings

4.6.5. Wireless Backbone Connectivity Solutions

In addition to supporting user devices, wireless networks can be used to deliver backbone network connectivity, particularly where a cabled solution is either not feasible or not cost effective. This can be used to connect remote, temporary and mobile buildings to the LAN in a school environment.

Two common ways of delivering wireless backbone connectivity are:

a) Point to Point (P2P) connections
b) Wireless mesh connections

4.6.6. Point to Point External WAPs

Point to Point (P2P) wireless connectivity using the 5 GHz band.

Many wireless suppliers have WAPs that can be deployed as P2P transmitter/receivers, and by using special directional antennae they can connect over distances in excess of 5 km (line of sight).

Point to point external WAPs shall have the following features:

a) Antenna minimum of 2x2
b) Wi-Fi 5 (5 GHz)
c) Integrated antenna
d) Minimum point to point throughput of 100 Mbps (PHY rate)
e) Be of the same brand as the internal WAPs for ease of management
f) Be protected against misalignment or physical damage from flying objects
g) Be IP 66 rated minimum
h) Be dual radio to allow local connectivity on one radio and bridging on the other.
i) Bridging shall be done using 5 GHz radio

4.6.7. Wireless Mesh

Using standard 802.11 technology, wireless vendors have developed proprietary routing protocols to create self-forming, self-healing resilient mesh networks in order to extend a LAN or connect devices such as VoIP or video equipment.

The wireless mesh technology chosen shall be capable of managing multiple on and off ramps to the wired network and be able to mitigate loops and broadcast traffic to maximise performance.

Meshing can be achieved by one of the two following methods and suppliers of WLAN equipment shall state what is supported by their WAPs.

a) 5 GHz is dedicated for backhaul and the 2.4 GHz radio for client access.

b) Support for client and backhaul on the same radios (Preferred).

The advantages of mesh technology are the same as with P2P but with the added benefit of resiliency and survivability. In a fully distributed mesh, no one node can take down the entire network as traffic is routed around the outage.

Disadvantages are generally performance. As wireless is a half-duplex shared medium, each mesh hop will result in a decrease in throughput unless dual bonded radio technology is used. In most cases the benefits of a resilient, flexible infrastructure outweigh any performance limitations.

The WLAN solution shall support WAP Meshing for self-heal and auto-fail over in the event of LAN link loss.

Recommend not turning WAP meshing on unless there are issues with LAN link loss as it can potentially cause other network issues.

4.6.8. Retention of Existing Wireless Access Points

The decision to retain or replace existing WLAN equipment shall be based on the following criteria:

a) WAPs that do not meet the Mandatory parameters detailed in Appendix 1 – **replace**
b) WAPs or WLAN solutions with no management function – **replace**
c) WAPs that are at End of Life (EoL), End of Sale (EoS), outside of warranty or are no longer supported – **replace**
d) WAPs that are compliant with the base feature sets outlaid in appendices of this document and not Wi-Fi 5 or 4x4:4 (5 GHz) and of the same brand as new WLAN equipment may be redeployed in appropriate locations at the network edge if compatible with the new solution – **redeploy/repurpose**
e) WAPs of the same brand, but firmware is incompatible with new WAPs or multiple instances of the control or management interface required to support them **- replace**

4.7. WIRELESS LAN MANAGEMENT AND SECURITY

Network security is critical to the reliable and safe functioning of a wireless network. Steps shall be taken to secure each device on the network, as well as securing the 'edge' where the internal network connects with other networks, such as the Internet.

The depth of security necessary in a school environment will vary, depending on the size of the school, and the way in which it uses its network.

This document uses the term security to cover the technical implications of a range of physical and logical security options. Access management is often described in terms of authentication, authorisation and accounting (AAA).

Security concepts are critical in defining the objectives of a wireless deployment project. Security and access management needs to be considered at all stages of WLAN implementation. Once the WLAN is running, it shall be monitored on an ongoing basis to detect and mitigate security and access risks. To assist with this, proactive event logging and notification shall be implemented.

4.7.1. Key Security Concepts

In a school network, security shall be applied to all WAPs. The security configuration is undertaken using the WLAN Management software to configure the Cloud Controller, which in turn propagates the configuration to the WAPs.

4.7.2. Device or User Authentication

Some authentication techniques authenticate the user of a device; others authenticate the device itself, regardless of who is using it.

Device authentication is simple to configure on a wireless network and when used with WPA3, can provide sufficient security for a school. Offering tight controls governing the specific wireless devices that are allowed to connect, such as limiting use to school-owned devices.

A school that anticipates widespread wireless use (such as BYOD) shall implement user authentication rather than device authentication. This is usually provided using the 802.1X protocol or via a Captive Web Portal if the device does not support 802.1X. Both 802.1X and Captive Web Portal are mandatory WLAN features.

These authentication methods use a database of authorised users (such as a school's existing directory service). The person connecting to the wireless network will enter their username and password to verify their identity.

Some vendors have additional methods of authentication based on the current standards such as Unique Per User Pre-Shared Keys, this is a highly desirable feature for client devices that don't support 802.1X.

4.7.3. MAC Address Filtering

A common technique used to authenticate a device is to use the device's Media Access Control (MAC) address. If the device attempting to connect to the WLAN has a MAC address that matches one of the allowable addresses then it is allowed to connect.

MAC address authentication is not a recommended access method (unless combined with other authentication techniques) for the following reasons:

a) While the MAC address is, in theory, unique to each device, in most wireless devices the MAC address can easily be 'spoofed', or changed. This makes it very unreliable for identification.
b) MAC address authentication adds additional overhead by requiring the administration of a database containing the MAC address of every device that is permitted to access the WLAN.

4.7.4. Pre-shared Key or Password

A network can be configured so that devices are prompted to enter a 'Pre-Shared Key' (PSK) before being allowed to connect.

This technique works well for small networks or networks where only school staff and school-owned devices are connected. This offers more security than MAC address filtering, but it is easy for a password to be 'shared' further than desired, for this reason PSK shall not be implemented on any device accessing a school network, unless they do not support any other wireless security. Ideally, the password should be changed regularly, but this can cause issues in securely notifying all users of the new password.

Innovations from some vendors use proprietary techniques to extend this authentication method to provide granular per-user PSK's in order to provide per-user Authentication and Authorisation.

Some devices might only be able to use less secure protocols. An example might be a hand-held barcode scanner that communicates over a wireless network and is used for tracking books in a school library. In this case, access shall be firewalled to communicating with one application only, with no Internet access or if they are third party IoT sensors that need to access the internet, they shall be placed into their own VLAN and the firewall pointed at the specific database needing access. Any device authenticated using a MAC address only shall be allowed access to its specific need only, as it is relatively easy to make any wireless device take over a connection set up in this way.

4.7.5. Encryption Techniques

Encryption is important in wireless networks as unencrypted wireless signals can easily be intercepted and 'read' by 3rd parties.

Early wireless systems commonly used Wired Equivalent Privacy (WEP). WEP is an encryption method that operates at Layer 2 based on the RC4 Cipher. WEP uses a static key and nowadays tools that can rapidly break (decrypt) the encryption used by WEP are easily obtained on the Internet, making WEP unacceptable for almost all wireless networks.

To overcome the security shortcomings of WEP, Wi-Fi Protected Access (WPA) was introduced in 2004 as an interim snapshot of the IEEE 802.11i security amendment (pending the development of WPA2). WPA only supports RC4 and TKIP dynamic key management and has a number of security vulnerabilities.

In addition to being well out of date, and providing low security, using WEP or WPA will limit the throughput of a wireless network. Both WEP and WPA shall be avoided. WPA2 was introduced in 2004 and provides strong encryption using the Advanced Encryption Standard (AES) using the CCMP encryption method and incorporates the mechanisms defined in the IEEE 802.11i standard.

WPA2 is provided in two modes. WPA2-Personal is based on Pre Shared Key passphrase authentication and WPA2-Enterprise mandates the use of 802.1X authentication with mutual validation.

WPA3 has now been introduced and provides further advances in security on WPA2; this is the industry accepted best practice for robust wireless security and performance, and shall be the security method implemented on a school network.

4.7.6. WPA2 Authentication

4.7.6.1. WPA2 Personal

WPA2 and Personal uses a PSK passphrase to provide authentication and authorisation. PSK authentication, works well for a home and small office network, but managing the shared key is difficult when there are many users and therefore this method shall not be used in schools.

4.7.6.2. WPA2 Enterprise

WPA2 Enterprise mandates the use of mutual user authentication and authorisation via 802.1X/EAP (Extensible Authentication Protocol) and while more complex to initially set up, this is the recommended approach for medium and large sized schools.

802.1X is a port based access control standard that restricts access to network resources until user authorisation has been completed.

There are various components to this framework, including the client device (Supplicant), Authenticator (AP) and Authentication Server (RADIUS server).

There are a variety of EAP methods, which can be confusing, and it should be noted that a number are proprietary to certain vendors.

The major factor to consider in selecting the appropriate method is that the method used on the client device (supplicant) and the Authentication Server (AS) shall be the same.

For example Microsoft Windows XP/Vista/Win7/Win8 support EAP-TLS, PEAP-TLS /MS-CHAP and are widely used for this reason.

The difference between TLS and MS-CHAP is the method in which user credentials are presented. TLS is based on Client and Server Digital certificates and requires a Public Key Infrastructure (PKI) in order to generate and manage the digital certificates. MS-CHAP is based on user name and password.

The reasons for the different methods are generally security based. It is technically harder to obtain a digital certificate than it is to obtain a user name and password via social engineering, therefore the industry best practice is to use EAP-TLS or PEAP-TLS with non-exportable certificates for client authentication however this may be impractical for some environments due to the administrative overhead it adds.

There are a number of Authentication Server options available. Examples are Microsoft Internet Authentication Services (IAS) and more recently Network Access Policy Services (NPS). These are services that are part of Microsoft Windows Server and are integrated into Active Directory.
Other network systems from Apple, Novell, or Linux can provide the 'RADIUS' protocol required for 802.1X/EAP.

4.7.7. WPA3 Authentication

4.7.7.1. WPA3 Personal

WPA3-Personal increased protection for individual users through provisioning of more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE), which replaces Pre-shared Key (PSK) in WPA2-Personal.

The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further network interaction. This method of Authentication shall not be implemented in schools.

4.7.7.2. WPA3 Enterprise

WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocols across the network.

WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data.

WPA3 shall be implemented as the standard for all school networks.

4.7.8. Captive Portal

The authentication techniques outlined above focus on controlling connection to a wireless network at the Data Link Layer (refer Glossary below for further reading).

A captive portal can offer some control and security by allowing any device to connect to a network at this lower Data Link layer, but then requiring authentication before the device can access the Internet or any network services.

With a captive portal, users typically cannot access anything until they start a web browser session and they are then redirected to a special web page called a Captive Web Portal (CWP) where they are required to enter a username and password before continuing further (this technique is often used to provide wireless access in airports, cafes etc.).

Captive portal can be provided either with or without Access Layer authentication (e.g. Open or with PSK). In the case of an Open SSID, the captive portal should be delivered via Secure Sockets Layer (SSL) in order to encrypt the user's credentials.

Authentication is typically queried against a centralised user directory in order to leverage existing user information. Common authentication methods include RADIUS, LDAP, and Active Directory. Once the user is authenticated, the services available to them will depend on what has been allowed by the school. In some

circumstances this might only be simple browsing or the ability to create a VPN to get more functionality with associated better security.

4.7.9. Wireless LAN Management

WLANs shall be managed, with either locally available embedded interfaces or via dedicated management system onsite, in the cloud or by third party providers.

A managed WLAN system may be monitored and modified using common management methods:

a) Command line interface (CLI)
b) Secure Shell (SSH)
c) Simple Network Management Protocol (SNMPv3)
d) Secure web interface via web browser (HTTPS)
e) Secured API (If applicable)

In most cases they should utilise an access control list and be matched to a trusted internal network IP address. For medium to extra-large schools, centralised management ability will result in significant savings in administrative time and effort.

Mandatory management features for the various switch types are provided in Appendix 1.

5. WIRELESS LAN SYSTEMS: TECHNICAL REQUIREMENTS

5.1. GENERAL

A variety of mandatory and desired system features have been tabulated in the appendices of this document to enable decision making with regards to system selection and deployment in schools.

5.2. WIRELESS ACCCESS POINTS

Most WAP devices will come in different shapes and sizes but will commonly have at least one copper 1 Gbps Ethernet PoE enabled uplink port to provide data connectivity back to the wired network and also to supply power to the WAP itself. As per Appendix 1, there are set minimum requirements as to what the WAP hardware and software must be capable of and this will dictate how the complete system will best delivery robust network connectivity to the various types of users and devices.

These WAP units, when installed shall be securely attached to the brackets where they are attached to the building and will not fall in moderate levels of building movement.

If there is an indicator LED light(s) on the unit, it shall be configurable and indicative of the status of the network at that location. This will aid in quick identification of faults by users.

Refer to Appendix 1 for a full set of technical requirements.

5.3. WIRELESS CONTROLLERS

Wireless controller appliances situated onsite, hosted by a third-party or cloud based controllers are implemented to provide a means of easily managing security and authorised access to relevant users. It is also used to manage RF aspects of the complete system to ensure RF signal strength, channel selection, roaming decisions are optimised so as to maintain user experience expectations.

There are many features required within the controller to maintain robust connections between the WAP and the devices needing high performing Wi-Fi connections. Please refer to Appendix 1 for all minimal technical requirements.

6. WIRELESS LAN SYSTEMS INSTALLATION PRACTICES

6.1. GENERAL

The WLAN system supplier/reseller or appropriately qualified designate that can supply all labour, materials and equipment required for installing, testing and commissioning the network.

The supplier or designate shall include a copy of all relevant specifications, compliance reports, documentation and diagrams including the WLAN IP address assignments for installation in an “as-built” document manual.

6.2. SAFETY

Any electrical work shall be carried out by a registered electrician to AS/NZS 3000, AS/CA S009, the Ministry of Education Electrical Infrastructure Policy and standard, the Ministry of Education’s ICT Cabling Infrastructure Policy and Standards for Schools and the Ministry standards are found at:
https://www.education.govt.nz/school/property-and-transport/suppliers/technical-information/responsibilities-of-an-ict-contractor/.

All contractors shall comply with the requirements detailed on the Ministry of Education website and are found at:
https://education.govt.nz/school/property-and-transport/health-and-safety-management/property-contractor-health-and-safety/

An IEEE 802.3 compliant transformer coupled with auto-sensing MDI and MDI-X ports may be an important consideration if UTP copper cabling is to be used to connect WAP to switches in separate buildings which have their own separate earth connections. This is to avoid electrical discharges created by electrical current imbalances across the two discrete electrical systems.

Installations shall comply with Electrical Energy Source (ES1, ES2 and ES3) requirements detailed in AS/CA S009 and a warning label shall be fitted to all accessible sides of a cabinet and outlet that is either ES2 or ES3 (Hazardous).

PoE switching shall not exceed the designed remote powering capability of the cabling system. If PoE switches are installed in a cabinet for remote powering purposes and no remote powering label exists on the cabinet, then the network switch supplier or approved ICT Contractor when installing any new network switching devices shall install a warning label on the front, back and sides of the cabinet. Detailing the maximum permitted remote powering as per the cabling manufacturer’s warranty and recommendation. The label shall comply with the requirements of the *Ministry of Education’s ICT Cabling Infrastructure Policy and Standards for Schools*.

All ICT contractors and Integrators installing PoE switching or patching fibre optic cabling shall have completed the '*Ministry of Education's ICT Cabling Infrastructure Policy and Standards for Schools*' approved contractors course to demonstrate competency in understanding the safety requirements for working with fibre optic cabling, remote powered systems and any network providing connectivity to safety devices e.g. Lockdown, CCTV, Panic Alarms (Security Intrusion Detection Systems) etc. The contractor's certificate shall remain valid for a period of two years from passing the exam.

All contractors maintaining a network containing fibre optic cabling and interfaces shall ensure all locations containing this equipment have compliant labelling installed by them if it is missing.

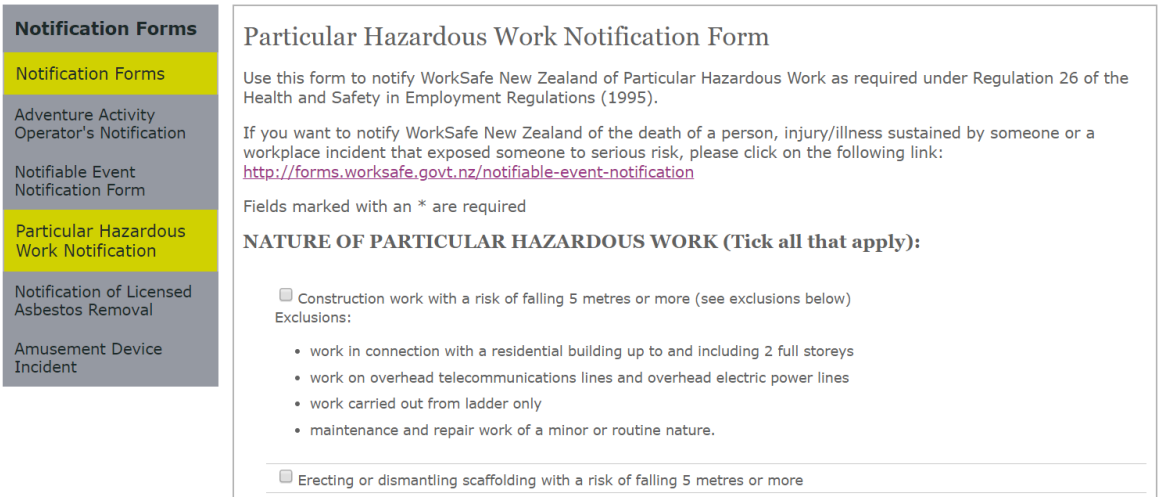
Any systems running on the network that are considered to be there for safety shall have an agreed uptime with the board of trustees and an appropriate UPS or other method of achieving this shall be deployed. Systems that may require this include; CCTV, Security, BMS, PA and Lockdown.

Any installation where the height of the installation is above 5m must be notified to Worksafe e.g. Gym's, Halls etc.

Worksafe: What is a notifiable work?

Under the Health and Safety at Work Act 2015 (HSWA) you must notify Worksafe when certain work-related events occur. A notifiable event is when any of the following occurs as a result of work: a death notifiable incident or injury notifiable incident.

WORKSAFE



6.3. MANUFACTURER'S RECOMMENDATIONS

All equipment shall be installed and performance tested in full accordance with both the manufacturer and distributor's recommendations and instructions.

6.4. DOCUMENTATION

The contractor that has supplied the WLAN shall produce both pre and post installation, a full network diagram with IP addresses and VLAN information detailed. Also required, within one week of the site visit, is a commissioning report and excel spreadsheet containing equipment serial numbers and a completed network switch site sign-off form from the school stating that the network and all existing services have been tested and are operational. It shall be the contractor's responsibility to demonstrate operational status to the school authorised contact.

All WAPs installed shall be clearly and logically labelled and all newly installed WAPs shall be documented with evidential photographs indicating position within a designated space prior to the installer completing the commissioning.

The commissioning report form shall include, at a minimum, the following information:

a) Key ports – ports of interest; switch link-ups and TOs
b) Interface check – all ports set to auto negotiate, full duplex, 1 Gbps or 10 Gbps where applicable
c) Rapid Spanning Tree Protocol (RSTP) status check – Root Bridge switch documented, RSTP turned on and Portfast / BPDU Guard enabled
d) Network Mesh test (If applicable) - Disconnect data uplink to check if meshing works.
e) Verify device configuration – final check of configuration for errors
f) WAP RF end to Core speed test – network core to edge throughput and latency tests from WAP to furthest wall within that designated space.
g) Internet speed test (Compare to N4L connection supplied)
h) IP address scan – a list of devices operating on the network at the time of scan

A backup of all device configurations shall be produced and retained by the school, with a copy remaining with the contractor that undertook the installation as a backup for a minimum of 5 years. Any of the original older WAPs retained after a network upgrade shall be reconfigured so as to be consistent with the newly installed WLAN equipment.

Any network configuration changes undertaken shall also comply with the backup requirements.

7. WARRANTY AND SUPPORT

7.1. GENERAL

The WLAN system supplier shall warrant that all products will operate to the standards and specifications claimed by the manufacturer and that the product is free from any defects in materials or workmanship.

The manufacturer or supplier shall make technical and user documentation on the product freely and readily available to the school.

7.2. MANUFACTURER'S WARRANTY

7.2.1. Hardware Warranty

The manufacturer shall provide a limited lifetime replacement warranty on the WAPs, controllers, other associated hardware. Warranty provisions shall include on-site repair or replacement and the supplier shall hold sufficient replacement stock in New Zealand to deliver a replacement unit to any school suffering a failure no later than same business day for Controllers and "next business day" for WAPs.

It is the expectation that assistance is guaranteed within two working days during the business week and in instances where workarounds are provided, a resolution will be carried out within five working days to the occurrence of the issue depending on severity.

Refer to Appendix 1 for mandatory hardware warranty requirements.

7.2.2. Software Warranty

The supplier shall provide limited lifetime software support on the WLAN system and free access to firmware upgrades within the firmware feature set purchased. Refer to Appendix 1 for mandatory software warranty requirements.

7.2.3. Service Level Agreements

Quotations for service support may include an option for a Service Level Agreement. In event of hardware failure the SLA shall stipulate within what time frame a replacement unit will be dispatched to the school and shall meet the minimum hardware and software warranty requirements. Premiums may be charged for service outside normal business hours.

Quotations may be formulated to include financial penalties for failure to meet the agreed SLA or Contractual Agreement.

8. QUALIFICATIONS

8.1. INSTALLER QUALIFICATIONS AND SELECTION

The specialist contractor engaged to supply, install, and commission the selected WLAN system shall be approved as a reseller and certified as an installer by the manufacturer or distributor of the equipment in New Zealand prior to commencing work on the installation. The specialist contractor shall also be capable of maintaining the selected WLAN system.

All ICT contractors and Integrators shall have completed the Ministry of Education's ICT Cabling Infrastructure Policy and Standards for Schools approved contractors course to demonstrate competency in understanding the safety requirements for working with fibre optic cabling, Remote powered systems and any network providing connectivity to safety devices e.g. Lockdown, CCTV, Panic Alarms (Security Intrusion Detection Systems) etc. The contractor's certificate shall remain valid for a period of two years from passing the exam and schools shall request a copy of the contractors certificate and expiry date.

When calling for tenders or requesting quotations schools should invite responses from resellers/installers who can provide documentation detailing their level of manufacturer/distributor certification together with the following information:

a) Company overview and profile
b) Copy of warranty certification statements from the manufacturer
c) Customer reference letters with contact details (three required)
d) Company staff details and number of certified engineers
e) Full-time staff & responsibilities
f) Part-time contractors & responsibilities
g) Training
h) Industry wireless specific training
i) Manufacturer/distributor certification held by the reseller/installer
j) Manufacturer certification held by the New Zealand supplier/distributor
k) Ministry of Education's ICT Cabling Infrastructure Policy and Standards for Schools approved contractors certificate number and expiry date
l) Health and Safety documentation
m) Type, make and model of testing equipment used, for example:
    - UTP and Fibre cable certification equipment
    - Traffic performance analysers
    - Packet capture and protocol analysis tools
    - IP addressing audit tools
    - Fibre cleaning tools utilised

Schools shall be accountable for ensuring contractors are suitably qualified and police vetted to work at their school. Police vetting requirements for contractors can be found at:

http://www.education.govt.nz/school/property-and-transport/projects-and-design/role-of-the-board/early-stages/police-vetting/

8.2. SUPPLIER QUALIFICATIONS

The New Zealand specialist supplier/distributor approved by the equipment manufacturer as a qualified supplier/distributor shall provide second level support services to the reseller/installer of the WLAN system.

The supplier/distributor shall maintain an engineering staff specifically to support their resellers. The engineering staff shall be certified to install and maintain the selected switching systems. The installer shall provide documentation detailing the level of manufacturer certification held by their supplier/distributor when submitting quotations and tender responses.

9. OTHER CONSIDERATIONS

9.1. HEALTH AND SAFETY CONSIDERATIONS

9.1.1. Hardware

All equipment capable of fibre optic connections shall be equipped with fibre terminal dust covers (or equivalent) to avoid accidental exposure to laser light.

These covers shall remain in place until such time as a cable connection is in place.

A warning label shall be installed requiring all unused fibre ports to have dust covers fitted and a warning label compliant to Clause 11.1.5.5 of AS/CA S009 shall be fitted by the contractor to the cabinet door when any equipment containing a fibre optic connection is installed within the cabinet.

9.1.2. Protection from Radiofrequency Electromagnetic Fields

The Ministry of Education acknowledges that the health and safety of children in our schools is of primary importance. As such it regularly monitors New Zealand Standards, international Standards and credible research on wireless technologies and radiofrequency electromagnetic fields as they become available.

Current advice from the New Zealand Ministry of Health states that:

> *The health research carried out to date shows that working and studying in areas with Wi-Fi equipment poses no health and safety risks to adults or children. Although no special precautions are needed, if individuals are concerned and wish to reduce their exposures, they can take simple steps to do so:*
>
> a) *Wireless access point shall be installed by a suitably qualified person and shall be installed as per the manufacturer recommendations.*
> b) *When working with a Wi-Fi enabled laptop, place it on a table rather than directly on the lap.*

For further advice about safe use of Wi-Fi in the workplace, please visit:

http://www.health.govt.nz/your-health/healthy-living/environmental-health/household-items-and-electronics/wifi-networks/

9.1.3. Peripherals and Other Systems

The following systems and peripheral components shall be considered in conjunction with the design and implementation of the switching system:

a) UPS system capacity requirements, accommodation, battery maintenance and life span (UPS required for safety systems running on the network, refer to safety section)
b) Wi-Fi enabled IP telephony handsets
c) Video conferencing systems
d) Multicast streaming systems
e) Access to the Internet and associated firewall
f) IoT Sensors or Triggers
g) Printers and printer servers
h) File servers
i) Equipment room alarms and climate control
j) Security and alarm systems (Contractor shall confirm in writing if any intrusion detection system functions run on the network and contain panic alarms, lockdown or other life safety applications and design accordingly)
k) Building management systems (Contractor shall confirm in writing if any BMS run on the network and are for safety purposes and design accordingly).
l) IP Hearing assist solutions

10. APPENDIX 1: WIRELESS LAN REQUIREMENTS

10.1. INTRODUCTION

The following technical specifications shall serve to inform vendors, wireless system integrators and schools of the minimum requirements when selecting a wireless network product suite.

This document forms part of the Ministry of Education School WLAN Standards Which can be found at:

https://www.education.govt.nz/school/property-and-transport/suppliers/technical-information/responsibilities-of-an-ict-contractor/

10.2. SYSTEM OVERVIEW

10.2.1. The Proposed System shall be:

a) From a single vendor
b) A purpose-built managed enterprise wireless system
c) From a vendor that can demonstrate sound financial status to address the risk of insolvency

10.2.2. The Proposed System WAP shall have at a minimum:

a) The ability to support Wave 2 MU-MIMO based Wi-Fi 5 on 5 GHz and Wi-Fi 4 2.4 GHz.
b) The ability to display users, laptops and general location of devices on a management console.
c) The functionality to support all current wireless standards including the older 802.11a/b/g and the Wi-Fi 4 standard in both the 2.4 & 5 GHz bands.
d) The ability to initiate rate limiting of individual SSIDs or user profiles (if individual user profiles are available on the management interface).
e) The ability to configure time-based access policies is a requirement for any compliant solution e.g. Student WLAN operates only between 8:30am – 3:30pm and Staff WLAN operates 24/7.
f) The ability to support various levels of QoS, at a minimum, 802.1p and DiffServ.
g) Access Points rated for 802.3af and/or 802.3at Power over Ethernet and defined in the product data sheet.

10.2.3. The Proposed System Controller shall have at a minimum:

a) A wireless system with a multi tenanted centralised hosted controller and management system providing segregation between tenants.
b) The centralised controller shall be hierarchical and have a minimum of 3 layers.
c) The management system shall have published API capability.
d) Concurrent dual radio 4x4:4 MU-MIMO (in 5 GHz) and 2x2:2 MU-MIMO (in 2.4 GHz) Access Points at a minimum.
e) Geographically diverse redundancy providing High Availability functionality for the centralised hosted controller system.
f) All parameters detailed as “Mandatory” in this appendix under sub-sections 10.3.1 to 10.8.2.

10.2.4. How to read these requirements

Legend:

Mandatory	M
Highly Desirable	HD
Desirable	D

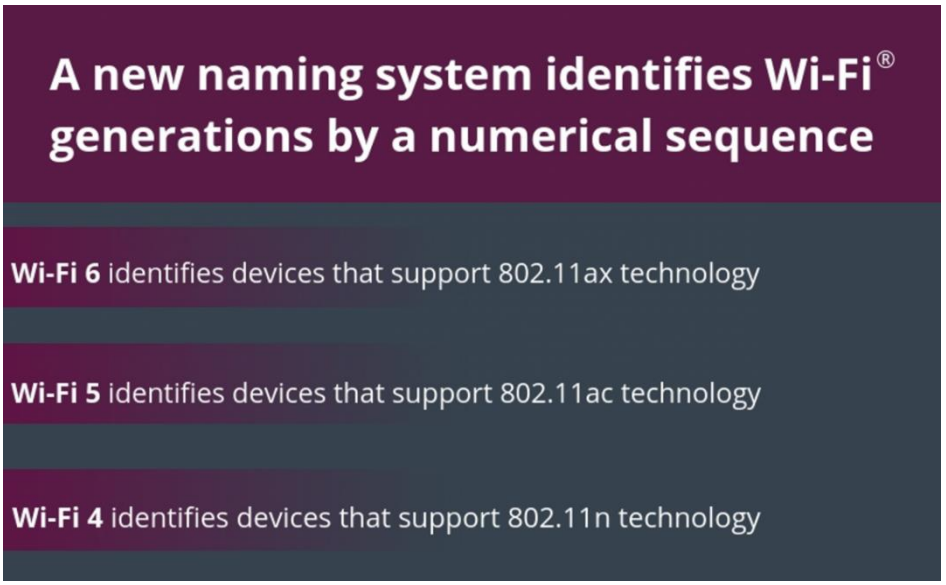
Note 1: Items listed that require a software license upgrade or additional fee to meet the Mandatory Ministry WLAN requirement shall be delivered fully enabled within any base switch unit.

Note 2: Copper and fibre connections are supplied via the appropriate SFP module. Core and distribution switches may need multiple SFP+ or N-Base-T ports to cater for 802.11ax or Wi-Fi 6 deployments. Designers and purchases of equipment shall take this into account when selecting a switch.

10.2.5. Changes in this Standard - Transitioning to the new naming convention:

References to the type of technologies that are to be supported by the solution will hence forth use Wi-Fi Alliance's definitions as per the below table.

https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6



10.3. WARRANTY AND SUPPORT

10.3.1. Hardware Warranty

Item #	System Feature	Importance
10.3.1.A*	The WLAN solution Hardware must have a Limited Lifetime Warranty on Cloud Controllers (if applicable) and Access Points.	Mandatory
10.3.1.B	Any newly deployed equipment shall not be End of Sale or End of Life (EoS/EoL) and shall have a minimum of 5 years operational life for the length defined in the hardware and software support period.	Mandatory
10.3.1.C	All newly deployed WLAN hardware shall include a Limited Lifetime Replacement Warranty for a minimum of 5 years. This shall be next business.	Mandatory
10.3.1.D	The Limited Lifetime period for hardware shall be defined as a minimum of 5 years beyond EoS/EoL for Hardware.	Mandatory

*Manufacturer shall stipulate whether a limited lifetime warranty also applies to all hardware components (e.g. SFP or expansion modules), fans (if applicable) and power supplies.

10.3.2. Software Support - Firmware

Firmware is defined as the internal operating system of the WLAN hardware.

Item #	System Feature	Importance
10.3.2.A	The WLAN solution shall have 5 year Support Licenses available for Cloud Controllers and Access Points, this shall be the minimum requirement for all newly deployed equipment.	Mandatory
10.3.2.B	Unlimited vendor Technical Assistance Centre (TAC) support shall be included for all newly installed WLAN equipment.	Mandatory
10.3.2.C	Security patches for known threat vulnerabilities shall be available for the duration of the limited lifetime warranty.	Mandatory
10.3.2.D	The Limited Lifetime period for software support shall be defined as a minimum of 5 years beyond EoS/EoL for Hardware.	Mandatory

10.3.3. Software Support - Management

Management software is defined as the external application used to manage the configuration and administration of the WLAN hardware.

Item #	System Feature	Importance
10.3.3.A	The LAN solution shall have 5 year Support Licenses available for all switching and routing equipment, this shall be the minimum requirement for all newly deployed equipment.	Mandatory
10.3.3.B	Unlimited vendor Technical Assistance Centre (TAC) support shall be included for all newly installed WLAN equipment.	Mandatory
10.3.3.C	Security patches for known threat vulnerabilities shall be available for the duration of the limited lifetime warranty.	Mandatory
10.3.3.D	The Limited Lifetime period for software support shall be defined as a minimum of 5 years beyond EoS/EoL for Hardware.	Mandatory

10.4. PERFORMANCE

10.4.1. Air Interference

Item #	System Feature	Importance
10.4.1.A	Conforms to all current applicable air interface standards for Wi-Fi including 802.11a, 802.11b, 802.11g, Wi-Fi 4, and Wi-Fi 5.	Mandatory
10.4.1.B	The WLAN system access points and cloud controller shall carry the Wi-Fi Alliance Wi-Fi interoperability certification at a minimum for IEEE 802.11a, 802.11b, 802.11g, Wi-Fi 4 and Wi-Fi 5. If the certificate is 'in process' the vendor shall state where the company is in the process and what sections are completed. It is not sufficient that a vendor's product be a member of the Wi-Fi alliance.	Mandatory
10.4.1.C	If some of the vendor's products are certified but not the product(s) being put forward the vendor shall supply a letter stating the reasons why that product(s) is not certified.	Mandatory
10.4.1.D	Conformance to the radio spectrum policies for spread spectrum devices operating in the 2.4 GHz band and 5 GHz bands. Please state all applicable certifications relevant to NZ so that your product complies with government regulations for radio transmitters and electromagnetic interference.	Mandatory
10.4.1.E	Frame aggregation support (MSDU/MPDU)	Mandatory

10.4.2. Access Points (AP) Internal

The integrate solutions shall be capable of performing to the highest level possible and as such, 4x4:4 (5 GHz) units are the minimum AP requirement.

Item #	System Feature	Importance
10.4.2.A	Each access point shall have a minimum of two radios able to operate concurrently, one radio assigned to 2.4 GHz operation, the other radio to 5 GHz operation. Access points with a single radio covering both bands are not acceptable.	Mandatory
10.4.2.B	The access point shall support Wi-Fi 5 Wave 2 operation in the 5 GHz band, and Wi-Fi 4 operation in the 2.4 GHz and 5 GHz bands concurrently.	Mandatory
10.4.2.C	Load balancing between: Access Points 2.4 GHz & 5 GHz radios on any given AP	Mandatory
10.4.2.D	Up to 8 SSIDs per radio to support tiered service architecture;	Mandatory
10.4.2.E	AP Meshing – ability to expand or bridge network via AP Meshing. Vendors must confirm if their Wi-Fi 5 compliant product supports this feature.	Highly Desirable
10.4.2.F	AP Meshing – The WLAN solution shall have the ability to self-heal and auto-fail in the event of LAN link loss.	Mandatory
10.4.2.G	Beam forming – Vendors must specify current provisions, whether it's chip or antenna based, and if the system beam forming is considered unique or proprietary.	Mandatory
10.4.2.H	Antenna signal gain (specify dB value and band)	Mandatory
10.4.2.I	Auto-channel selection	Mandatory
10.4.2.J	Additional features such as Maximal Ratio Combining (MRC) and Cyclic Delay Diversity (CDD). Vendors must specify additional features when proposing at solution.	Highly Desirable
10.4.2.K	Distributed intelligence (i.e. Fat APs)	Highly Desirable
10.4.2.L	Adaptive resource management (i.e. air time allocation) to fairly manage legacy and current client devices	Highly Desirable
10.4.2.M	Omni-directional antennae	Mandatory
10.4.2.N	Band Steering ability based on client	Mandatory

Item #	System Feature	Importance
10.4.2.O	Must be capable of installing on a wall, ceiling or ceiling grid without any decrease in RF performance	Mandatory
10.4.2.P	Wi-Fi 6 is desirable only if the hardware can be guaranteed to be compatible with the ratified standards due near June 2020, where software updates can bring full compatibility up to standards compliance post June 2020. Vendors must state compliance and compatibility if putting forward a Wi-Fi 6 solution.	Highly Desirable
10.4.2.Q	Access points shall have the ability to concurrently serve at a minimum 150 devices per access point and shall be configurable within the management interface.	Mandatory

10.4.3. Antenna

Shall support all other features unless specifically indicated:

Item #	System Feature	Importance
10.4.3.A	The number of antennas must be 4x4 MU-MIMO minimum on the 5 GHz and 2x2 MU-MIMO on the 2.4 GHz radio.	Mandatory
10.4.3.B	The number of spatial data streams on the 5 GHz radio must be four (for 1733Mbps 5 GHz and 300mbps 2.4 GHz PHY rate per radio).	Mandatory
10.4.3.C	Access Points must be capable of running MU-MIMO on all radios.	Mandatory
10.4.3.D	External mount Access Points with integrated antennas must be IP66 rated minimum.	Mandatory

10.4.4. WLAN Roaming

Item #	System Feature	Importance
10.4.4.A	User equipment shall be able to seamlessly roam from one access point to another fast enough to provide a voice conversation on a Wi-Fi connection, inside the specified coverage zones.	Mandatory
10.4.4.B	Must provide intelligent support for clients that do not support roaming tendency settings, or are either too “sticky” or too “loose” with their AP association.	Mandatory
10.4.4.C	Users shall not have to reconnect to the network when they roam from one area to another within the campus coverage zones.	Mandatory
10.4.4.D	Mobile devices shall not have to re-authenticate as they move from access point to access point.	Mandatory
10.4.4.E	The wireless system shall support 802.11k, 802.11r and 802.11v.	Mandatory

10.4.5. Centralised Controller Solution

Item #	System Feature	Importance
0.A	A wireless system with a multi tenanted centralised hosted controller and management system providing segregation between tenants.	Mandatory
0.B	The centralised controller shall be hierarchical and have a minimum of 3 layers.	Mandatory
0.C	The management system shall have published API capability.	Mandatory
0.D	Ability to share licence blocks between multiple cloud controllers (if applicable)	Mandatory

10.5. SYSTEM FEATURES

10.5.1. VLAN and Policy Support

Item #	System Feature	Importance
10.5.1.A	The wireless cloud controller and access points must provide IEEE 802.1q VLAN support.	Mandatory
10.5.1.B	The solution must be able to support all existing VLANs in the air without changing any existing router configurations, adding any new routing protocols to the network, or modifying any client configurations.	Mandatory
10.5.1.C	Enforcement of VLANs via WLAN management policies.	Mandatory
10.5.1.D	Enforcement of existing network policies including access control lists (ACLs), class of service (CoS), quality of service (QoS) and routing policies.	Mandatory
10.5.1.E	The WLAN system must provide user-to-user traffic isolation, even if they are on the same VLAN or on the same AP or across multiple AP's.	Mandatory

10.5.2. Ethernet Support

Item #	System Feature	Importance
10.5.2.A	Access points must comply with IEEE 802.3, for Wi-Fi 5 10/100/1000 Mbps Ethernet and Wi-Fi 6 Access points 10/100/1000/2.5G/5G Ethernet.	Mandatory
10.5.2.B	The connection between the access point and the controller (if applicable) and or the Ethernet network must comply with 802.3 specifications. Proprietary line protocols are not acceptable as access points must interface with Ethernet switching equipment.	Mandatory
10.5.2.C	All access points shall be powered by open standards based network switch ports compliant with 802.3af and if required, 802.3at/bt. If the proposed hardware requires 802.3at/bt for full functionality, then the minimum PoE requirement for full functionality shall be stated.	Mandatory

10.5.3. Traffic Management

Item #	System Feature	Importance
10.5.3.A	The WLAN solution shall have the ability to choose traffic pathways e.g. ability for traffic to be tunnelled via controller (if applicable), or direct to gateway from WAP	Mandatory
10.5.3.B	Shall support a minimum of 60 concurrent clients on a single multicast stream per WAP.	Mandatory

10.6. SECURITY

10.6.1. Encryption

A significant requirement is the breadth of security measures supported by the proposed WLAN system. The following requirements are designed to determine standards adherence, range of security protocols supported and future-proofing of the system.

Item #	System Feature	Importance
10.6.1.A	The WLAN system at a minimum shall support the following encryption types: a. WEP with 64-bit and 128-bit encryption b. WPA/WPA2 (TKIP and AES-CCMP) with pre-shared keys c. WPA/WPA2 (TKIP and AES-CCMP) with 802.1X. d. WPA3 The vendor shall also state any client number limitations that exist per WAP for each encryption method. **Note**: As well as having speed limitations, WEP and WPA are not recommended choices from a security perspective and shall be avoided. WPA2 will be the minimum acceptable encryption protocol for all new WLAN implementations.WPA3 has now been introduced and provides further advances in security on WPA2; this is the industry accepted best practice for robust wireless security and performance, and shall be the recommended security method implemented on a school's network.	Mandatory
10.6.1.B	The catch-all encryption requirement is that the WLAN system shall comply with 802.11i in addition to the above. Wi-Fi alliance certification is required for WPA3 and the above authentication methods.	Mandatory

10.6.2. Authentication

Item #	System Feature	Importance
10.6.2.A	The WLAN system must support IEEE 802.1x authentication.	Mandatory
10.6.2.B	The WLAN System should have a RADIUS proxy function available	Mandatory
10.6.2.C	The WLAN system must support MAC-based authentication.	Mandatory
10.6.2.D	The WLAN system must support web-based authentication (captive portal).	Mandatory
10.6.2.E	The WLAN system must support the following Extensible Authentication Protocols (EAP): EAP-TLS, EAP-TTLS, PEAPv0-MSCHAPV2, and PEAP-TLS.	Mandatory
10.6.2.F	The WLAN system must support bonded authentication, tying the device together with the authenticated user.	Mandatory
10.6.2.G	Device OS fingerprinting – ability to offer network features based on device OS.	Highly Desirable
10.6.2.H	Authentication mechanisms used by client varies greatly; at a minimum vendor's solutions shall be able to authenticate against: I. RADIUS (Window and open source versions) II. Active Directory (AD) III. LDAP IV. OpenLDAP V. eDirectory VI. Azure AD VII. Google	Mandatory

10.6.2.I	Ability for the Cloud controller to integrate with cloud based authenticate services.	Mandatory
10.6.2.J	Ability to support other out-of-domain users and devices.	Highly Desirable

10.6.3. Wireless Intrusion Protection, Detection (WIPO/WID) and Counter Measures

Item #	System Feature	Importance
10.6.3.A	Active background rogue AP detection service, with automated emails to the administrator upon identification	Highly Desirable
10.6.3.B	Stateful Firewall	Highly Desirable
10.6.3.C	Implement counter-measures to address rogue APs	Highly Desirable
10.6.3.D	Ability to identify and disable Peer-2-Peer networks	Highly Desirable

10.6.4. End Point Integrity Checking - Network Access Control

Item #	System Feature	Importance
10.6.4.A	Product contains NAC functionality, or can integrate with a NAC solution.	Highly Desirable
10.6.4.B	Part of a certified partner program with a NAC device. Please provide details.	Highly Desirable
10.6.4.C	Does your NAC solution use a software agent or is it an agent-less solution?	Highly Desirable
10.6.4.D	Remediation via quarantine or captive portal	Highly Desirable

10.6.5. Guest Access and Control

Item #	System Feature	Importance
10.6.5.A	Ability to generate and manage guest users on the network via a unique Pre-Shared Keys	Highly Desirable
10.6.5.B	Captive portal available	Mandatory
10.6.5.C	Network Address Translation protocol for deployment in Proxy/TMG server environment (or statement of how your system deals with Proxy/TMG server)	Highly Desirable

10.7. SCALABILITY

10.7.1. Expansion

Item #	System Feature	Importance
10.7.1.A	The WLAN solution must provide a Linear licensing mechanism that allows 1:1 purchasing of Access Points and Licenses	Mandatory
10.7.1.B	The WLAN solution must provide a “Plug and play” approach that allows end users to plug in new Access Points and pick up configurations automatically, also referred to as “zero-touch configuration”	Mandatory
10.7.1.C	The WLAN solution shall have the ability to set up remote offices or satellite locations with access points and centrally manage them to allow staff and students to seamlessly move between locations.	Mandatory

10.7.2. IPv6 Support

Item #	System Feature	Importance
10.7.2.A	The WLAN solution shall provide IPv6 support in both the cloud controller and Access Points.	Mandatory

10.8. MANAGEMENT

The WLAN solution will provide a wireless management interface for Moves/Adds/Changes as well as WLAN network wide monitoring.

10.8.1. WLAN Management Software

Item #	System Feature	Importance
10.8.1.A	Visibility and management of all WLAN equipment: Cloud Controller and Access Points	Mandatory
10.8.1.B	Secured Web GUI	Mandatory
10.8.1.C	Visibility of WLAN users and their devices on the network	Mandatory
10.8.1.D	Visibility of WLAN users: i. User name ii. IP address & MAC address iii. Roaming history iv. Bandwidth usage v. Location (to nearest AP at a minimum) vi. Equipment 'host name' if resolvable	Highly Desirable
10.8.1.E	Visibility of RF Performance	Mandatory
10.8.1.F	Event Logging i. Administrative audit trail ii. Uptime iii. Rogue AP detection iv. Detection of RF Interference	Mandatory
10.8.1.G	Critical incident email reporting	Mandatory
10.8.1.H	RF Planner	Highly Desirable
10.8.1.I	Spectrum Analyser	Mandatory
10.8.1.J	Visibility and management of security features	Mandatory
10.8.1.K	Ability to support REST API functionality	Highly Desirable
10.8.1.L	Ability to detect De-Authentication events	Mandatory
10.8.1.M	The WLAN solution must have the ability to export the configuration of a site at that moment in time allowing it to be stored for system recovery purposes. The solution shall permit the configuration to be stored with the Ministry of Education, along with as-built documentation as a backup.	Mandatory
10.8.1.N	The WLAN solution must allow functional survivability of the local access points to deliver authentication and transportation of user traffic if an outage occurs at all cloud controller(s).	Mandatory
10.8.1.O	Syslog support	Mandatory

10.8.2. Users and SSID

Item #	System Feature	Importance
10.8.2.A	Time-based access policies per SSID	Mandatory
10.8.2.B	User-based WLAN policies to throttle or restrict access	Highly Desirable
10.8.2.C	Options to adjust SSID visibility	Mandatory
10.8.2.D	Guest functions*	

* Refer to Guest Access & Control, section 10.6.5.

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Published by the New Zealand Ministry of Education, July 2020.

Ministry of Education
Mātauranga House, Level 1, 33 Bowen Street,
Wellington 6011, New Zealand.

www.education.govt.nz

Copyright © Crown 2020
This publication is subject to copyright. Apart from any fair dealing for the purpose of private study, research, criticism or review, or permitted under the Copyright Act, no part may be reproduced without the permission of the Ministry of Education, New Zealand.

ISBN: 978-1-77663-720-1 (Online)