MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Technology in Schools

School Wireless LAN Guidelines:

Understanding Wireless Guide

Version 1.2

May 2015

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 this guideline. In particular, the assistance of the following parties is acknowledged:
Torque IP, Connector Systems, Allied Telesis, NSpire Technologies Ltd.
New Zealand offices of Ruckus Wireless, Aerohive, Aruba Networks.

Table of Contents

1 Introduction

This document is part of the Education Infrastructure Service: Technology in Schools, School Wireless LAN Guidelines 2015. It 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 infrastructures for New Zealand schools. The document addresses deployment of wireless access to computer networks in New Zealand schools in a way that is complementary to existing wired infrastructures.

Overall, the Guidelines aim to inform in the following areas:

- What is wireless LAN (a brief description)
- How do wireless LANs work
- What are the benefits of wireless access
- Current wireless access technology and standards (technical details)
- Overview on deployment of a wireless LAN (planning, installation and integration, and avoiding problems)
- Product and integrator selection
- Security issues, threats and standards

The Guidelines will be updated as standards change. Prior to using this document please confirm that it is the latest version. The latest version of each of the Guideline documents may be obtained at www.education.govt.nz/ict-standards

1.1 Audience

There are two documents that make-up the wireless Guidelines, please see the documentation map below.

This document is the Understanding Wireless Guide. Its purpose is to provide guidance to principals, board members, and others wanting an introduction to the issues around selecting and procuring wireless LAN technology for their school.

The Understanding Wireless Guide introduces the overall concepts of a Wireless LAN, and summarises the content required when commissioning an RFP process.

1.2 Documentation Map

The Education Infrastructure Service: Technology in Schools, School Wireless LAN Guidelines 2015 consists of three documents:

1.2.1 School Wireless LAN Guidelines – Understanding Wireless Guide

This document – described above.

1.2.2 School Wireless LAN Guidelines – Building and Maintaining a Wireless Network

For a school IT support person who is implementing and maintaining a school wireless LAN (WLAN). This document outlines the standards available for building and securing a WLAN, technical considerations for implementation, and requirements for ongoing maintenance.

1.2.3 Recommended Specifications for School Wireless LAN Systems

Intended to provide guidance for the selection of wireless network technologies and features.

1.3 List of Acronyms

This list simply expands all acronyms used in this document. The glossary at the end of this document includes definitions.

Acronym	Stands for
AAA	Authentication, Authorisation and Accounting
AP	Wireless Access Point
BYOD	Bring Your Own Device
COW	Computer on Wheels
ICT	Information and Communication Technology
IPv6	Internet Protocol Version Six
LAN	Local Area Network
LMS	Learning Management System
N4L	Network for Learning
NIC	Network Interface Card
PC	Personal Computer (in the context of this document, can be desktop or portable)
RFP	Request for Proposal
SSID	Security Set Identifier
TELA	Teachers Laptop Scheme (run by Ministry of Education)
WAP	Wireless
WLAN	Wireless Local Area Network
WNIC	Wireless Network Interface Controller
WPA2	Wi-Fi Protected Access version 2
802.11i	WPA2

1.4 Scope

The Schools ICT LAN Infrastructure Standards and Guidelines Project aims to inform schools as they make changes to their Information and Communication Technology (ICT) infrastructure.

In Scope	Outside Scope
Wireless networks supporting learning and research within schools	Community Wireless which might be based around a school
General considerations for wireless network installation	Use of wireless technologies for point to point connections between buildings
Wireless connection between a 'user device' and the school network.	Detailed connectivity between school LAN and WAN
Additional security required for a school wireless network	General school network security, including firewall configuration and other network issues
	Bandwidth management of external Internet access
	Teaching pedagogy required to make use of an expanded wireless network.
	Selection of, and management of, wireless devices, beyond connection to the network.
	Detailed specification of a school Wireless Network RFP.

2 What is a WLAN?

A WLAN (also known as WiFi or Wi-Fi) enables those using portable devices in a school to connect to the school computer network without needing a network cable. Typically, it is used to connect devices such as laptops, netbooks and tablet computers (including iPads), and other devices such as some phones and iPod devices. Desktop PCs can also have a wireless adapter added to them to enable connectivity to a WLAN.

New Zealand schools generally have an Ethernet computer network used to connect to the Internet, as well as services such as printing, and file sharing. The size and needs of a school should dictate the range of services available from their computer network.

Wireless networking has become common throughout schools within New Zealand, and in many other countries. The extent to which wireless networks are implemented varies widely, from small ad-hoc access in parts of a school, to almost half of New Zealand schools indicating they have a school-wide wireless network.

A number of schools have mapped a path to pervasive wireless coverage over their campus with the goal of supporting a 'bring your own device' (BYOD) environment. This environment will require a school-wide wireless network, which may be implemented in stages. The effectiveness of a BYOD environment can be enhanced by the provision of teaching resources that can be accessed both within and from outside the school

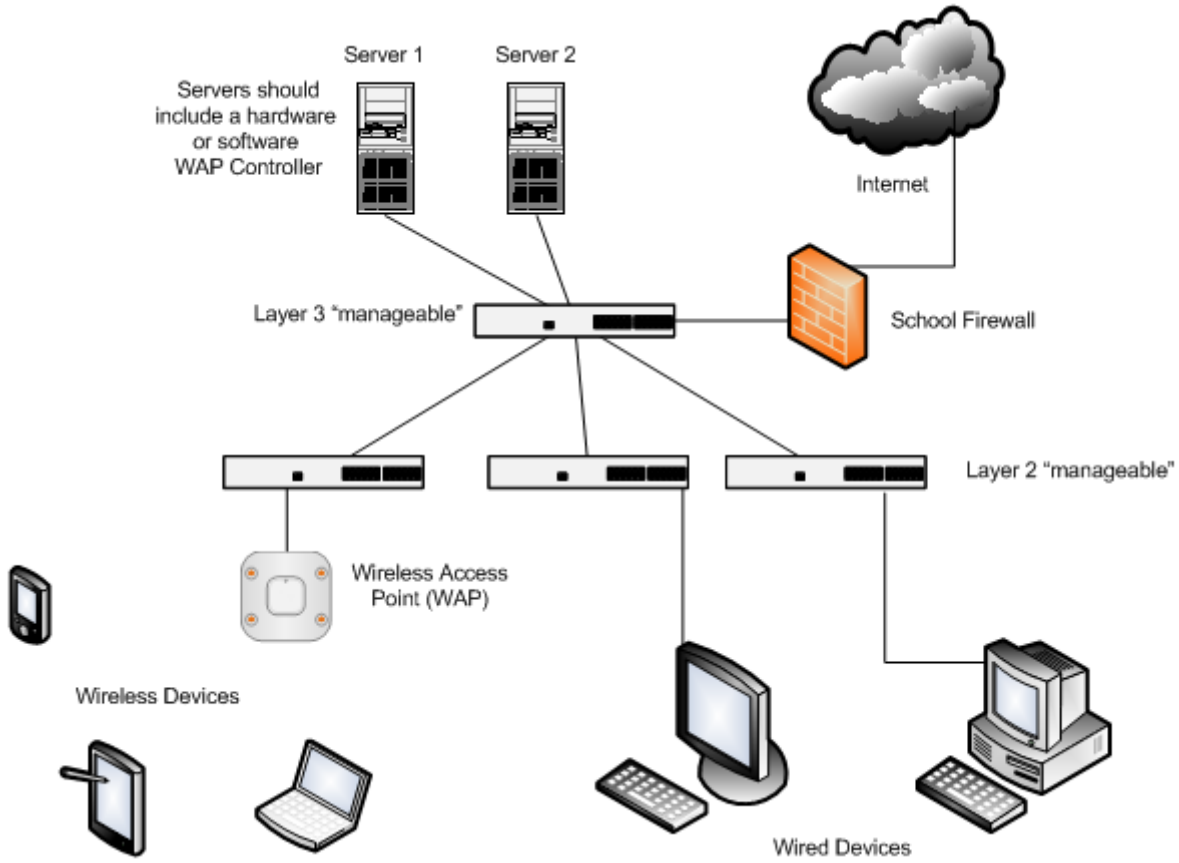
The first consideration before implementation or upgrade of a wireless network is to look at what the network is going to be used for in the short and medium term (typically five years into the future). Further discussion on planning a school's WLAN is in section 5.

Wireless networking uses many acronyms. A glossary of terms is included at the end of this document.

3 How does a WLAN Work?

In a wired network the network interface card (NIC) inside the PC provides an interface to the wired Ethernet local area network (LAN). A network cable connects the NIC to a wall data outlet/Ethernet port, which is wired to a port on an Ethernet switch. The Ethernet switch establishes a connection to the network services such as file and print servers, web proxy and e-mail servers, and to networks external to the school such as the Internet.

Figure 1 – Simple Network for Small School, with Wireless Access



A wireless network is composed of the same components as those used in a wired network except:

- The NIC is replaced with a wireless NIC (WNIC), usually integrated into the hardware in a wireless device.
- The network cable is replaced with a radio connection.
- The wireless (AP), which communicates with the WNIC by radio frequency signals, is connected to a data outlet/Ethernet port.
- Some form of wireless network management device/system is recommended for most schools. It can be software running on an existing server, a separate server, or in the "cloud" (on an external server typically accessed via the internet). Wireless network management devices/systems provide remote management of APs, can provide historical reporting, provide visibility of users on the WLAN and enable control over their activities/access.
- The wireless infrastructure should be capable of supporting a number of different networks simultaneously. There might be separate networks for staff, students and visitors, or some other arrangement appropriate to a particular school. The different networks would typically have different services available and different security safeguards – for example there may be a "guest" network that allows access to the Internet only and cannot reach any school file servers,

printers etc. Each different network will have a name – this is called the Security Set Identifier or SSID. The SSID is usually the network name your device will find and display when you search for a wireless network to connect to.

A diagram of the parts of a network, from the teacher to the Internet, is included following the glossary at the end of this document.

4 What are the advantages and disadvantages of a WLAN?

The New Zealand Government is supporting school connections to Ultra-Fast Broadband (UFB), which will also provide access to the Network for Learning (N4L). This increases the emphasis on schools to ensure that N4L and many other online resources can be accessed and used effectively. The implementation of a wireless network is one way to increase connectivity to these resources as it opens up the potential for BYOD.

Wireless networks come with both benefits and risks, some of which are described here.

4.1 Advantages

Some of the advantages offered by wireless network access are:

- Mobile access for learners' and teachers' devices. All laptops provided under the laptops for teachers and principals programme (TELA) since 2004 have integrated wireless network interface cards (WNIC's). Most portable network devices (laptops, netbooks, tablets, iPods, games consoles, etc) have integrated wireless access.
- Learners can access school and wider sourced material from any location where the wireless network is available.
- As more teachers use ICT to facilitate learning opportunities, learners can access those opportunities without the need for extra physical cabling. The networked device can be moved around to match learning needs, rather than ICT resources being tied to where there is a cable.
- If schools choose to increase the number of computers, or the places where they are used, this can be done with minimal additional cabling i.e. one cable run for each additional wireless , rather than one cable run for each computer. One can support multiple computers.
- LAN coverage can be extended to areas which are difficult or not cost-effective to cable. Examples include heritage buildings, remote buildings, temporary re-locatable classrooms, open plan areas such as halls and libraries and outdoor areas. See Appendix A in Building and Maintaining a Wireless LAN for further reading.
- A well designed and implemented wireless LAN gives schools the opportunity to provide Internet access to visitors to their campus with low risk and minimum investment.

4.2 Disadvantages

The decreasing cost of components and apparent ease of installation presents a compelling argument to "go wireless", however there are a range of issues to consider:

- Connecting a single wireless and providing a wireless service to a few laptops is a relatively simple task and requires few technical skills, but when a school needs to manage a larger number of wireless s then installation, integration and management becomes more complicated.
- While the file transfer speed ('data rate') of wireless has increased significantly over the years, wired network speeds have increased too. High bandwidth activities are still best done on wired networks.
- As the number of devices using a particular AP increases, the data transfer rate to each device will decrease accordingly. An AP has a fixed maximum amount of data throughput, if an AP is heavily used e.g. video content, large file transfers, or a large number of users; this will affect the bandwidth or data transfer rate (speed) available to all users connected to that AP. This situation can be mitigated by installing more s in high density use areas.
- Devices will only operate at a limited distance from an AP, with the distance largely determined by the wireless networking standard used. Obstacles between the AP and the user (e.g. walls, glass, water, trees and leaves) can also determine the distance of operation. Poor signal

reception has been experienced around reinforced concrete school buildings; these may require higher numbers of APs which in turn increases overall cost.

- As wireless standards change, it may be necessary, or at least desirable, to upgrade to higher specifications of wireless which could mean replacing wireless equipment (AP and wireless NICs) which may prevent the use of some older user devices. Currently, wireless standards are changing more quickly than wired standards.
- Wireless network traffic is half-duplex which means transmission and receipt of information cannot happen at the same time. Wired Ethernet is full-duplex which means transmission and receipt of information occurs at the same time, therefore offering faster performance.
- Data speeds drop as the user moves further away from the AP.
- Wireless LAN technologies operate in the unlicensed portion of the radio spectrum where there is no formal process for preventing interference caused by other wireless network installations or from the multitude of other wireless devices designed to operate in the same frequency band. Well known sources of conflict include microwave ovens and 2.4GHz (usually older) cordless phones plus other nearby WLAN's. This interference will become more of an issue as more wireless devices are deployed. Proper planning, monitoring and management of a wireless network will help mitigate the impact of interference.
- Security, at a variety of levels, requires more complex design and configuration to mitigate risk.

In practice, a wireless LAN on its own is not a complete solution and will still require some copper cabling to be in place to provide a network backbone. For a very small school, this might only require one cabinet containing two or three devices and cabling to each classroom.

5 Planning for a Wireless LAN

5.1 The Evolving Requirements of Wireless Access

School wireless networks have evolved from being predominately ad-hoc deployments in small areas, through becoming part of school-wide infrastructure, to BYOD deployment where staff and students expect the network to always work in all parts of the school campus. Early WLAN deployments focussed 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 proliferation of mobile devices (particularly smartphones, iPads and tablets) is pushing the demand for faster and more reliable wireless networks, Users typically have multiple apps on their devices that often download updates as soon as they are connected to a WLAN, they upload increasingly higher resolution photos and videos to the cloud and to social media applications, and they regularly view videos on YouTube and other websites,

Schools' circumstances vary. This needs to be reflected in the planning, design and procurement processes for a wireless LAN to specifically meet the needs of an individual school. This section describes some of the key planning and implementation steps.

5.2 School ICT Ecosystem

Some requirements that need to be considered before deploying a wireless network are the school's network strategy and how the network will support educational aims.

One method of ensuring technology choices align with the school's Strategic Plan is to use an IT Investment Management Framework.[1]

Where a requirement or need is identified to assist learning, a Business Case is written collaboratively by educators and IT staff. The business case outlines the drivers for change, objectives and benefits and identifies the enablers of change (usually technology). The enabler of change could be the WLAN network for example.

The Business Case is assessed by a Governance Group for its alignment to the schools Strategic Plan. It is then prioritised, budgeted and implemented or not, according to where it sits in the priorities of the Strategic Plan.

Once a business case is implemented it becomes a project which can be completed and closed only once the technology is selected, installed, tested and delivering on requirements. Prior to project closure a support and maintenance plan and a review cycle should be in place. This review usually aligns to the IT hardware lifecycle but also includes a review to ensure the service/technology is still meeting the original objectives.

Following a methodology such as the IT Investment Management Framework will help to ensure IT investments are well thought out, cost-effective, and support the missions and education goals of the school.

[1] Defined in the glossary at the end of this document

5.2.1 Planning Considerations

When planning a wireless network to deliver educational outcomes for a school, the requirements should be carefully defined. Asking the question, "what do we want to deliver by installing a WLAN" and then breaking this down into specific questions will greatly assist a school in identifying important factors. A comprehensive and clear set of requirements will assist with both the product and integrator selection process. It can also provide the school with some measurables/deliverables they may wish to see demonstrated should they request a proof of concept prior to final product selection.

Planning factors to consider include:

- **Who:** which members of the school community will use the wireless network? Some options might be staff only, staff and just a few devices per classroom, groups of laptops that will be moved from class to class, only certain years of students permitted BYOD, or BYOD for all students (where some students may have more than one device). Will guests and visitors to the school be catered for? Should there be separate networks available for different types of users e.g. staff, students, guests etc.?

- **Where:** what areas of the school need to have have wireless network available? Are outdoor areas included? Will the entire campus be covered from the outset or will it be a staged approach? A site plan of the campus and floor plans for buildings (to scale) are useful planning tools and will be required for the WLAN design. What are the school's future plans for growth/new buildings over the next five years?

- **When:** should the network be available 24/7? Should access be turned off after hours and during weekends etc.? Do boarding students require access after school hours?

- **How many:** understanding the location and density of users on a wireless LAN is critical to proper planning. It is essential to define not just the total number of users expected on the wireless network but where they may be located (e.g. if wireless network coverage is required for a large library or lecture theatre it must allow for the expected density of users in this space). What are the school's plans for growth in student and teacher numbers over the next five years?

- **What type of devices:** having a good understanding of the types of devices the network needs to support is important (netbook, laptop, tablet, smartphone etc.). It may be that a school develops a policy of supporting a select number of different types of school owned client devices including Computers of Wheels (COWs) and Teacher Laptop Scheme (TELA) laptops or it may be an open BYOD policy. When considering selection of, or policy for, BYOD client devices it is important to consider the devices' WNIC capabilities (i.e. 802.11 a/b/g/n/ac, 2.4GHz and 5GHz) and whether the devices will support the method of network access that the school wishes to implement (e.g. captive portal, pre-shared key or some other method). In each case appropriate access and security policies can be crafted to match the device policy. The wireless performance of client devices can vary greatly – generally influenced by the strength of their antenna – and it may be worth further consideration when developing a device policy. Low strength antennae in client devices may result in more APs being required.

- **What network-based applications and services[2]:** what should the WLAN users be able to access/do once connected? Some options might be Internet access only, Internet and the school

[2] Defined in the glossary at the end of this document.

LAN access, file sharing and printing, or all of these and also support for streaming video and voice applications. A school needs to be mindful that deploying a WLAN with Internet access may significantly impact on Internet usage. A review of the schools Internet service is advisable at the time of deploying the WLAN – including assessiing what connection speed to the Internet is required and whether data should be capped or unlimited.

- **How will access be managed:** what usernames and passwords will be required? There are many options, and the final decision may be dependent on which applications and services need to be made available and which device type is in use. This is covered in detail in Section 3 - Security and Access Management in the "Building and Maintaining a Wireless LAN" guideline document.

- **How critical is the wireless network:** once installed and integrated into the school in daily use, how critical would an outage to the wireless network be? If very critical then planning needs to address the issue of redundancy and resiliency of the wireless network.
- **What impact will the school's physical environment have on wireless:** Careful consideration must be given to the construction materials of the school buildings, the topography of the site and potential sources of external interference such as large, multi-function radio towers or other nearby wireless networks. It is important when planning to clearly identify issues particular to the school site such as temporary classrooms, remote buildings, relocatable buildings and special use buildings that will require special attention when planning the wireless network. See Appendix A of the "Building and Maintaining a Wireless LAN" guideline document for further reading.

- **How will the WLAN be supported after installation:** a decision needs to be made as to whether the school's IT staff will support the WLAN network or whether it will be outsourced to the integration company or elsewhere. WLANs do need ongoing monitoring as the usage patterns change with time and this can dramatically affect performance. See 5.3 Operational Expenditure and 5.4.2 Ongoing Support for further reading.

Defining and detailing the school's requirements, either in the RFP process or with the selection of integrators the school chooses to work with, forms the basis of the key deliverables the wireless network needs to meet. In larger and/or more complex WLAN deployments it may be prudent to run a Proof of Concept stage to ensure the selected product performs against the school's requirements. See the "Building and Maintaining a Wireless LAN" guideline document for further detail.

5.3 Costs of a School's Wireless Investment

Advantages and potential uses of a wireless network were outlined in section 4 above. Alongside those considerations, a school should consider the costs of installation and use of a wireless LAN.

When considering information technology investment, all costs need to be projected over the lifetime of an asset including the up-front investment and on-going costs. Establishing the 'Total Cost of Ownership' in this way will minimise unforeseen expenses and complications. When budgeting for wireless technology the following factors should be quantified:

- Capital Expenditure:
    - Installation and hardware costs: WLAN components include APs, controllers/management systems and additional computers or other devices that might be needed as part of the project. Cabling and power supply costs should also be factored in. Costs vary widely depending on a school's needs.

- Other implementation costs: may include fees for experts contracted as part of procurement for services such as a WLAN design and site survey and for integration of the WLAN into the wired infrastructure.

- Operational Expenditure:
  - Maintenance, support and upgrades and monitoring: As with most information technologies, deployment of wireless networking will involve additional work for school IT, management and administration staff. Some of the extra work includes access provision, monitoring the wireless performance, security monitoring, managing upgrades as new options are rolled out, and physical maintenance of the wireless equipment. A school should consider whether they wish to insource or outsource (or a mix of both) the on-going management and maintenance of the WLAN. Most WLAN solutions also have annual licensing costs that can be a significant part of the total cost.
  - Training and professional development: Although a good implementation of wireless technology means that users need little technical training to get connected to the network, technical staff managing the network may require training and support to stay up-to-date on the technology choices, security protocols etc. Teaching staff may need training and support in the use of new technology and in developing their e-Learning strategies and abilities.

5.3.1 Budgetary Considerations:

Wireless LAN deployments can vary greatly depending on the requirements of the school.

It should be assumed that one would need to be deployed for each co-located classroom and one for each isolated classroom.

Additionally schools should consider the requirement gathering costs, RFP or vendor selection costs, project management/co-ordination costs, ICT costs for internal network changes (IP addressing, firewall, VLANs, Active Directory, Radius etc) and ongoing support costs. Some or all of these may be undertaken internally or outsourced.

5.4 On-going Operational Support Considerations

After the completion of a wireless installation, there will be further considerations during operation of the network. This section describes on-going considerations.

5.4.1 On-going Security

Security is always a balance between risks (perceived and actual) and mitigation costs. Various factors need to be considered including the vulnerability of the network, the threat of attack, the value of the data to be secured and the costs involved. Wireless networks are often perceived as particularly vulnerable because anyone with a suitable wireless device can detect the presence of a wireless LAN. Some risks are specific to wireless, but in general a security plan that provides good protection to a wired network will also mitigate many risks from wireless. Securing WLANs, as with all networks, needs to be seen as a continuous process rather than a one-off step. Any security solution needs to be consistently and properly implemented with regular monitoring.

The wireless LAN should be configured so that anyone trying to gain access has at least the same access restrictions as they would if they sat down at a wired network workstation. Schools should be implementing a comprehensive security policy and incorporating best practices standards such as 802.11i.

5.4.2 On-going support of the WLAN

In planning for the operational on-going support, maintenance and management of the WLAN it is important to understand the requirements for uptime or availability of the network and the process for resolving issues. These requirements, processes and timeframes should be defined in a service level agreement.

This support could be provided internally by IT staff at the school or outsourced to an external provider.

A maintained list of Ministry approved wireless network integrators can be found at www.education.govt.nz/ict-standards

5.4.3 Online User Safety

Providing pastoral care to ensure the wellbeing of users is an important consideration in deploying WLAN. Many schools will already have a support structure in place to help develop confident, safe, and responsible online activity. This needs to be reviewed and extended, to cover specific issues with wireless devices, such as having less control over where and when a device is used.

Netsafe is a valuable resource to help with this. Netsafe provide a downloadable kit for schools to help students learn to stay safe online, and offer the www.myLPG.org.nz site, which contains a range of online content, covering current areas of online safety.

Schools may wish to incorporate an Acceptable Use Policy or Digital Citizenship practice.

5.5 Procurement

As wireless network technology has matured there has been a proliferation in manufacturer offerings in both equipment and management tools. It is important to understand that different vendors may offer solutions with technical points of difference. Consideration should be given to the vendor's architecture, hardware, software and management tools and how that meets the school's requirements and budget.

It is recommended that offerings from multiple vendors are sought and combined with quotations from a number of wireless system integrators is sought to provide the best end result in accordance with the school campuses individual needs

5.5.1 Integrator Considerations

The initial planning for a wireless LAN is critical in defining the requirements for selection of a suitable product and integrator. In creating a WLAN plan the school should clearly identify their requirements as per 5.2.1 and select both a product and an integrator who meets these requirements. A Proof of Concept prior to full install may be useful in cases where the requirements are complex to ensure the appropriate choice has been made. The integration company should be responsible for the physical installation of the wireless infrastructure, installing the management systems and integrating the solution into the wired network. Once installed the integrator should test and demonstrate that the installed product functions fully, delivers to the school's requirements, provide a guarantee period (in addition to the hardware/software product warranties) for any adjustments to the network configuration and performance (e.g. a 90 day guarantee period).

The integrator should provide copies of all relevant specifications, operations, credentials and management user manuals for the system and software and "as built" documentation. The integrator should also offer a basic training plan that covers all aspects of the network management that the school is taking responsibility for.

5.5.2 Guidelines for a Wireless Network RFP

Any purchase of a significant asset for a school requires technical knowledge. A wireless network RFP can be outsourced to consultants who will manage the entire process, and guarantee the quality of the resulting network. In some cases a school will choose to manage their own RFP process. Setting out the process to manage an RFP is out of the scope of the School Wireless LAN Guidelines.

An RFP document should clearly define the schools specific requirements that responders need to meet. This includes information about the school environment and the planning considerations as described above.

Some of the information a school would require from a response to an RFP is outlined below:

- A wireless design should be included in the response. This should cover how the solution will integrate with the wired LAN, how the solution will address security, authentication, location planning, and a site survey. Many wireless vendors are able to provide a predictive plan ("heat map") of the wireless coverage based on the wireless plan and then post-installation can provide a heat map of actual coverage.
- The response should indicate how the s will be cabled, installed and powered.
- The response should include an overview of all products available (for potential future requirements) and which products are being offered in this response. There needs to be a clear statement of the specifications of the products offered, including evidence that the requirements have been met. It should include antenna(e) used by the suggested products, with documentation supporting this information.
- The response should describe how the system will be monitored and managed day to day (e.g. by a WLAN controller or Network Management System). It should also indicate what level of visibility this system will provide (e.g. visibility of all s and client devices), connection speeds available to client devices, RF performance, security settings and how rogue s are handled.
- The response should describe all security options available from the product offered, and work required to implement and maintain security.
- The response should describe support for multiple VLANs, seamless client roaming, mesh support and support for future technologies such as IPv6.
- The response should include an explanation of how the solution proposed supports different device operating systems such as Windows, Apple (IOS/OSX), Linux, Android, and other client devices.
- The response should clearly address pricing for all options and, where applicable, licensing costs for three and five year terms.
- The response should describe the scaleability of the proposed wireless network, including what steps need to be taken to grow from the proposed number of s to the estimated future number of s and whether the solution is linearly scalable or stepped.
- The response should describe the resilience and redundancy of the proposed wireless network (e.g. , if an , controller or network management system fails what is the effect on the network and users).
- The hardware vendor should provide information on mean time before failure (MTBF) on their products.

In addition to any licensing costs, and dependent on the school's plan for managing the wireless network, the response should cover support options available from the integrator for an outsourced solution (what levels of support are available, what are response times, and examples of costs for specific and common support issues).

6 BYOD Considerations

Many schools are considering BYOD options where students are able to bring their own devices and connect them to the school's wireless network. This has substantial educational benefits for both teachers and students, but does have an impact on the network.

Some considerations that need to be taken into account for BYOD are listed below. Note that this is not intended to discourage schools from BYOD, rather it is to highlight some areas that may otherwise be overlooked in planning for BYOD.

- What BYOD devices will be supported? The greater the variety of devices, the more difficult support can become. Also, some older, or low quality, devices may slow the wireless network performance for other users.
- Have user densities been properly planned? If a large number of students concentrate in one area (e.g. a school hall) and all simultaneously try to use their wireless devices, the APs in that area may be overwhelmed. Typically deploying BYOD will require additional APs in a school. As a very rough rule of thumb, for a typical school with no BYOD, one AP per two adjacent classrooms may be suitable, while with BYOD one AP per classroom would be more likely.
- Is the school's IP Addressing scheme able to support the number of new devices? Each device that connects to the network needs an IP address. When the school's current IP addressing scheme was developed it may not have envisaged the number of devices that BYOD may introduce and so it may be inappropriate and need changing. This is not a trivial task for a large IT environment.
- What content filtering will be implemented? Consideration needs to be given as to what restrictions need to be placed on Internet activity, especially by students, and how this will be achieved. Should students be able to access social media sites (e.g. Facebook) and upload photos and videos to cloud storage?
- What controls should be placed on when BYOD devices can access the internet? Should students be able to access the internet (and other services) during lunchtime, after school etc.?
- Is the current Internet usage plan adequate? The introduction of BYOD may result in a substantial increase in Internet bandwidth usage. This is particularly so if applications like Skype, websites like YouTube, and social media access are permitted. It is important to ensure this increased usage has been budgeted for if the internet plan is not a flat rate plan.
- Will mobile phones also be allowed to connect to the network? All smartphones, and many other mobile phones, have wireless cabability and need to be considered in a BYOD policy. It is likely that many students will have both a tablet (e.g. iPad) and mobile phone that could be simultaneously connected to the WLAN, if permitted. This has implications for IP addressing and support, also some mobile phones have low specification wireless capabilities and can have a significant detrimental effect on the performance of other wireless users on the same AP.
- What Authentication, Authorisation and Accounting (AAA) level is appropriate? What authentication is appropriate to enable BYOD devices to access the network; once the network access is permitted what will the users be authorised to do; and what accounting information is required on what they have done?

7 Health Concerns

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 Wi-Fi technology and radiofrequency electromagnetic fields as they become available.

Current advice from the National Radiation Laboratory (part of the New Zealand Ministry of Health) states that:

> *The health research carried out to date shows that working and studying in areas with WiFi 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:*

- *Place the wireless up on a high shelf or away from where people might sit and work.*
- *When working with a WiFi-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

8 Glossary of Terms

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.
10GbE	10 Gigabit (per second) Ethernet.
1GbE	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.

Term, Acronym, or Abbreviation	Definition
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. 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 to 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 with 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.

Term, Acronym, or Abbreviation	Definition
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 must 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.
Band Steering	Some wireless vendors have developed band steering. This is the ability for an 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 5Ghz radio to ensure maximum performance for that client and to reduce the likelihood of the 2.4Ghz radio becoming overloaded.

Term, Acronym, or Abbreviation	Definition
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 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 must 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.

Term, Acronym, or Abbreviation	Definition
BSS	Basic Service Set Part of the 802.11 standard service set – the Basic Service Set refers to the communication between a single wireless and a wireless station.
Building backbone cabling	Cable that connects the building distributor to a floor distributor
Building distributor	A device (typically a 10/100 Mbps or 1Gbps 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 gigabit 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 users 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 3080 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 3080 class e 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.

Term, Acronym, or Abbreviation	Definition
Channel	Each frequency range used by 802.11 wireless (2.4GHz and 5GHz) is split into channels each of which each a subset of the frequency range. For example, the 2.4GHz band (used in 802.11b, g, and optionally n) is divided into 14 channels. The frequency (mid-point) of each 2.4GHz channel is 5MHz away from the frequency of the next channel (with the exception of channel 14 which is 12MHz away from channel 13). **2.4GHz Channels** Not all 2.4GHz 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 20MHz channel width, adjacent channels overlap and cause interference with each other. To overcome this, it is recommended that only channels 1, 6 and 11 be used as they do not overlap. **5GHz Channels** In the 5GHz frequency range there are far more channels specified in the IEEE standards, but again the allowable channels varies by country. The 5GHz channels that are permitted in most countries are typically 20MHz apart so there is no channel overlap using 802.11n in the lower speed 20MHz mode. But if channel bonding is used for higher speed a 40MHz channel is needed so there are issues with channel overlap. With 802.11ac the channel width required can be up to 160MHz for the fastest data speeds, so channel overlap becomes a significant design consideration.

Term, Acronym, or Abbreviation	Definition
Channel Bonding	Channel bonding is a technique where adjacent contiguous 20MHz wireless channels are combined into a wider channel to enable higher data rates. Channel bonding is typically only used in the 5GHz range as there are insufficient non-overlapping channels available in the 2.4GHz 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 20MHz channels to form 40MHz, 80MHz and 160MHz channels. The 160MHz channels can be either two adjacent 40MHz channels or an "80+80" configuration where two non-adjacent 80MHz 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 54Mbps). 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 20MHz 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 20MHz or 40MHz). For a 20MHz stream the maximum data rate is 70 Mbps while for a 40MHz stream it is 150 Mbps. So for 4 streams over a 40MHz 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 20MHz, 40MHz, or 80MHz and Wave 2 includes 160MHz). For a 20MHz stream the maximum data rate is 96 Mbps, for a 40MHz stream it is 200 Mbps, for an 80MHz stream it is 433 Mbps and for a 160MHz stream it is 867 Mbps. So the maximum combined data rate for a Wave 1 AP with 4 streams over an 80MHz channel is 1.73 Gbps and the maximum combined data rate for a Wave 2 AP with 8 streams over a 160MHz 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.

Term, Acronym, or Abbreviation	Definition
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 (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.
Encryption	The process of transforming data using an encryption cipher in order to render the data stream unreadable except with the key.
Floor distributor	A device (typically a 10/100 Mbps or 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 '2.4GHz' 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 humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.

Term, Acronym, or Abbreviation	Definition
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.
IETF	The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935.
IPSec	IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement VPNs.
ITIM Framework Information Technology Investment Management Framework	A framework developed by the United States General Accounting office, it can be used for both assessing the maturity of an organisations investment management process and as a tool for organisational improvement. http://www.gao.gov/new.items/d04394g.pdf
L2TP	The Layer Two Tunneling Protocol (L2TP) provides a dynamic mechanism for tunneling Layer 2 (L2) "circuits" across a packet-oriented Layer 3 data network (e.g., over IP). L2TP, as originally defined in RFC 2661, is a standard method for tunneling Point-to-Point Protocol (PPP) [RFC1661] sessions. L2TP has since been adopted for tunneling a number of other L2 protocols. L2TP is largely used with VPN access technologies.
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 amongst APs.
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.

Term, Acronym, or Abbreviation	Definition
Ministry	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. 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-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.
PCI	PCI (Peripheral Component Interconnect) is a local bus standard developed by Intel Corporation for attaching hardware devices (typically PCI cards) to a computer.
PCMCIA	PCMCIA (Personal Computer Memory Card International Association) is a standard for small, credit card-sized devices, called PC Cards to connect to computers to add functionality.
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.
P2P	Point to Point.

Term, Acronym, or Abbreviation	Definition
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).
PTP	Point to Point.
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. 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.
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.
SFP	Small Form-factor Pluggable (connector).
SNMP	Simple Network Management Protocol.
SNUP	School Network Upgrade Project http://www.minedu.govt.nz/snup
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 must 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.
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 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.

Term, Acronym, or Abbreviation	Definition
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: • Standard data traffic including staff • Other school-owned devices • Visitor wireless access • Student wireless access (BYOD) • Management of network devices • VoIP Phone connections • Streaming video, or video conferencing • 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.
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	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. 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 a secure (encrypted) private network created over any other (often unsecure) network.
WAP	Wireless Access Point

Term, Acronym, or Abbreviation	Definition
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 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.

9 End to End Network Diagram

The diagram below depicts an end to end network diagram of a school's network that includes a WLAN.

Note: Where Network for Learning (N4L) is available for a school's internet connection, a web and application layer firewall and content filtering system is available through the cloud on an opt-in basis. This could reduce infrastructure complexity and ongoing costs for the school by obsolescing the requirement to purchase and manage these systems independently.

Figure 2 – End to End Network