N4L

He horo ake, he haumaru hoki te ipurangi mō te ako

Faster, safer internet for learning

Kia ora

Network for Learning (N4L) is a Crown-owned tech company that connects 2,500+ schools and kura across Aotearoa New Zealand to faster, safer internet for learning.

We're one of the largest broadband networks in the country, meeting the connectivity and cybersecurity needs of 900,000+ ākonga and kaiako.

But we're more than just the internet - we're here to connect, protect and support schools to provide a safer online learning environment, so kaiako can focus on teaching and ākonga can focus on learning.

We Connect | Tūhono
Faster, safer, fully funded internet with uncapped data for state and state-integrated schools and kura across Aotearoa New Zealand.

We Protect | Tiaki
From filtering and firewalls, to email protection and segmented networks, our solutions and security experts help keep ākonga safer online.

We Support | Tautoko
Dedicated support teams and self-service tools help schools enjoy reliable access to a safer and more secure online learning environment.

Connect to faster, safer internet

We provide fully funded internet for all state and state-integrated schools and kura.

Our faster, safer internet includes uncapped data - meaning your school can use as much internet as you need to support teaching and learning. We also provide a secure Wi-Fi connection throughout the school grounds.

We design a network based on your school's needs, actively manage the connection and continue to develop new ways to make it safer and more secure.

With reliable internet, kaiako can focus on teaching and ākonga can access more ways to learn.

Upgrading your school's Wi-Fi

As part of the Ministry of Education's Te Mana Tūhono programme, we're working to upgrade school network equipment across Aotearoa to ensure a safer, more seamless Wi-Fi experience. We'll contact your school before the Equipment Replacement and Secure Access process begins, and we'll then support you through each phase of the upgrade.

1 Equipment Support

We provide support and assistance to ensure your wireless equipment continues to run smoothly until your equipment can be replaced as part of the upgrade.

2 Equipment Replacement

We work with you to design your school's network, order the required equipment and then install the wireless technology.

3 Secure Access

We're making your school's Wi-Fi more secure by making sure everyone has the right level of access to devices and content.

We do this by creating separate networks for staff, students and guests, with each user requiring a unique, authorised login to access their network. This gives everyone on your staff and student networks an identity, providing control of those accessing your network at all times.

Combined with network segmentation, an identity-based authorisation means your school will be less vulnerable to security breaches and online threats, providing improved protection of your school and student data.

Good to know

Internet speed and bandwidth utilisation is dependent on the number of users online, what is being downloaded, the devices used in your school and the school's wireless network performance. All these factors need to be taken into account as this will impact the speed that any single user can achieve.

Protect ākonga online with our help

Schools and kura are able to access a suite of fully funded safety and security services to help protect ākonga online. We combine our security solutions with people power and expertise to give you the confidence you need.

- ✓ **Built in protection** creates a strong protective foundation
- ✓ **Proactive detection** identifies vulnerabilities to stop threats in their tracks
- ✓ **Expert guidance** helps to improve your security posture, or to resolve or mitigate threats

Get a baseline level of online protection

Safe & Secure Internet makes it simple for your school to have a baseline level of online protection. It's a suite of five services with recommended settings, designed to help keep your ākonga safer online and your network more secure. We also monitor these settings and can let you know if something changes that could put your school at risk.

Firewall

The firewall acts as a wall between the internet and the school's network, allowing the good stuff through and keeping the bad stuff out. It prevents a huge amount of online threats and malicious activity from reaching school systems and devices.

Web Filtering

Our Safe & Secure Internet service includes Web Filtering, which helps block inappropriate websites and applications - including search engine websites that don't offer SafeSearch. We can block entire internet categories (e.g. games), specific websites or particular apps, and filtering rules can be customised for your school. Our Web Filtering also helps to block known Virtual Private Networks (VPNs).

It's important to understand that N4L's Web Filtering blocks websites and URLs, but not specific content within a website. As an example, we know YouTube is widely used to support learning. Our filtering only currently allows schools to either block or allow access to YouTube as a whole, but not individual videos based on inappropriate content.

This is where other technology solutions can play a role. YouTube offers filtering for content, and Google schools can manage their own settings in Google Workspace.

We've got some guidance around this on our website and we strongly recommend that schools and their IT providers make themselves aware of this.

Category filtering

We can block entire internet categories that are unwanted by your school, or we can block specific websites within a category. As part of our recommended settings, there are 17 web filtering categories that are the minimum categories we recommend that all schools block, and there are additional categories or websites schools can block at their discretion (e.g. social networking).

Application filtering

Similar to category filtering, we can block the use of unwanted apps within your school.

Customised filtering

Customised filtering allows us to apply a specific filtering policy to different groups of users, and at different times of the day. It requires each user group to connect to a different wireless network, e.g. senior students, junior students and staff each connect to a separate network.

Blocking Virtual Private Networks (VPNs)

We do our best to block known VPNs as they can be used to bypass your school's filtering or security, but unfortunately no solution can be 100% successful. If a new VPN is discovered at one school, our network can block this same VPN from being used at another school - which means we're continuously improving our ability to block known VPNs.

DDoS Protection

A Distributed Denial of Service (DDoS) attack is when a network gets deliberately bombarded causing it to slow down or crash, preventing legitimate users from accessing resources on the network or the network itself. DDoS Protection identifies and mitigates malicious DDoS activity before it impacts your school. This is automatically included as part of every school's connection.

DNS Threat Protection

This is an additional layer of protection that helps to further block unwanted content and minimise the impact of online threats (such as malware, ransomware and phishing scams) by preventing access to malicious websites.

SafeSearch

SafeSearch filters out adult content in search results from Google and Bing – it's enabled by default when schools use our DNS Threat Protection.

> **Good to know**
>
> We don't have visibility of a school's Google or Microsoft settings, so schools should work with their IT support person to review and update them.

Recommended settings

As part of our Safe & Secure Internet service we encourage schools to have recommended settings in place. To help maintain a baseline level of protection, we monitor these settings to make sure nothing has changed with the firewall or filtering settings, and if DNS Threat Protection is switched on.

It's up to school leaders to decide the settings that best suit the needs of your school. To learn more about these settings head to **n4l.co.nz/settings**, or if you'd like to discuss your settings with us please get in touch.

Web Filtering
With all recommended categories & websites blocked

+

Firewall
With recommended settings applied

+

DNS Threat Protection & SafeSearch
Enabled

> ## Keen to know more?
>
> To learn more about Web Filtering and online safety, head to **n4l.co.nz/onlinesafety**.
>
> You can also call us on **0800 LEARNING (0800 532 764)** or email support@n4l.co.nz if you'd like to review or change your school's Safe & Secure Internet settings.

Additional options to strengthen your protection

To protect ākonga online even further, schools can choose these additional options.

Mail Relay for group communication

This enables you to securely send large volumes of external emails to keep in touch with whānau and the school community. Our Mail Relay will securely check all outbound emails are free from spam and viruses before sending them on their way.

Remote Access for kaiako

With Remote Access kaiako have a secure way of accessing your school's onsite network regardless of where they are. This means they can work anytime, from anywhere. It also aligns with the Ministry of Education's security guidelines for remote access.

Email Protection for enhanced security

To help protect schools from the increasing number of email-based cyber threats, we offer an industry-leading inbound Email Protection solution. It's fully funded for eligible schools by the Ministry of Education and it works together with your school's existing Microsoft or Google email services.

Any school, regardless of size, can be a potential target to attack and should have increased levels of protection in place. Email Protection provides an enhanced level of email security for added peace of mind. You also have visibility of blocked emails via the Email Protection tool in MyN4L.

How Email Protection works

247.2 million Total inbound emails	**149.9 million** Emails blocked by Email Protection	**94.3 million** Emails delivered to school's service	School's settings **block** further emails	Safe emails **delivered** to school users

*Numbers above are based on emails received by users at ~1,500 schools over a single school term.

Switch on Safety for remote learning

We've created a free filter to protect ākonga when they're learning remotely. It means their device won't have access to certain sites that are deemed unsafe or inappropriate for learning. This includes a range of gambling and adult sites, plus sites known to host malware and phishing scams. To learn more visit **switchonsafety.co.nz**.

"If N4L hadn't been there, then who knows what could have happened? It was picked up, sorted and didn't require any intervention on our part."

Mark Hurley, St Mary's College

Cybersecurity services

- **Proactively monitor** your school network
- **Notify you** of cybersecurity vulnerabilities or incidents
- **Support you** to resolve any identified risks or issues
- **Quickly** and **efficiently** block local and global threats across the network

We've enhanced our cybersecurity network services by integrating with the National Cyber Security Centre's (NCSC) Malware Free Networks® service and Phishing Disruption Service™. This threat intelligence capability allows N4L to quickly and efficiently block local or global online threats across the network in near real-time. Schools automatically benefit from this at no cost and without any action required.

What are we looking out for?

- *Incidents*

    A cybersecurity incident is a bit like having an intruder on your property, and our Security team is the friendly neighbour who alerts you. Types of incidents we can identify and notify you about include:
    + Phishing - where cyber criminals attempt to trick you into revealing sensitive information or downloading malicious software.
    + Compromised email or login credentials.
    + Unusual or high risk remote traffic into your school's network.
    + A device that's infected with malware.

- *Vulnerabilities*

    Like a broken lock on your door, a vulnerability is something that has an exploitable weak spot. As part of our Cybersecurity services, we carry out regular scans of the network to see what might be accessible on the internet and if there are any potential security risks to schools or kura. If we see your school has serious vulnerabilities we'll work with you to remediate them.

- *Security improvements*

    We'll help with overall improvements to your network configuration, system firewall rules and email security to better protect you.

Good to know

It's **important to remember** that there's no way to guarantee 100% protection from online threats or inappropriate content. There are other actions your school can take to help keep your online learning environments safer and more secure, such as promoting digital citizenship and making sure appropriate security measures are in place.

The Ministry of Education has helpful information about keeping your school network secure and **Netsafe** has some resources on online safety, which we highly recommend checking out!

> "N4L support is always quick to respond, and very proactive. I appreciate when they have noticed something is wrong and get in touch with us to let us know, particularly when it's during the holidays or the weekend, when we aren't there to notice ourselves."

Evelyn Perry, Makara Model School

What happens if we discover a threat?

If we discover your school is exposed to a threat that could put you at risk, we'll notify you and your IT provider as soon as we can. We may contact you in different ways depending on the threat level, urgency and action required. We'll then work together to understand what actions need to be taken to mitigate the risk and support you with any remediations that may be needed. If you don't have an IT provider, that's okay! Our team can work with whoever you recommend is the best person for your school, or we can put you in touch with one in your area.

Advisories

We also provide security notifications called advisories. Advisories highlight the current cybersecurity threats and vulnerabilities that could impact your school, and offer guidance on how to mitigate their impact. If it's critical, we'll send the advisory to schools that we think could be impacted. Any active advisories can be viewed on our Alerts page on our website.

What happens if an incident has already occurred?

Whether you discover an incident or we do, we're here to help. If we believe your school has been impacted we'll let you know. Our team will be available to support you, your IT provider and other stakeholders (e.g. cyber insurance providers) as required to help investigate and remediate the incident. Afterwards, we'll provide you with a detailed incident report.

What more can I do to protect my school?

- Check your school is part of the Ministry of Education's **Risk Management Scheme** on their website. The scheme includes cybersecurity insurance.
- Sign up to **Email Protection**, which enhances your protection against spam and phishing attacks - and it's fully funded by the Ministry of Education.
- Ensure our Safe & Secure Internet **recommended settings** on page 7 of this brochure are enabled to provide a baseline level of online protection.
- Follow the **National Cyber Security Centre's (NCSC)** advice on other important steps you can take and critical controls you can implement in your day-to-day environment.
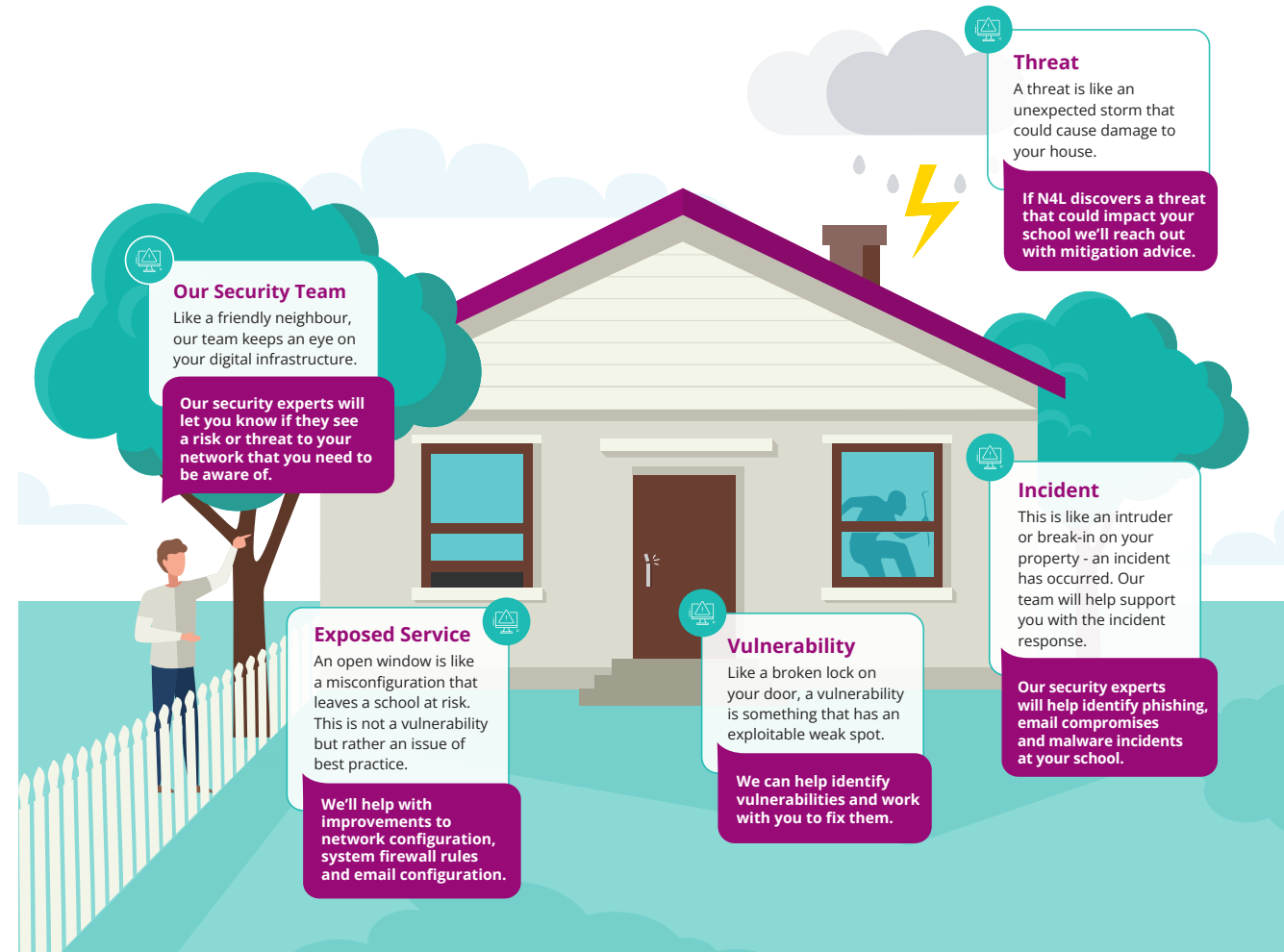- Check out the **cybersecurity tips** on the Ministry of Education's website.

Good to know

It's important we have up to date contact information for your school or kura so we can get hold of the right person quickly if there's a security incident. This includes your principal, IT lead and IT provider.

Explaining our Cybersecurity services

Here at N4L we have a wonderful team of security experts who are dedicated to supporting schools. Below is an illustration to explain some of the common cybersecurity terms you might hear from us about, and how our team helps in each scenario.

Threat
A threat is like an unexpected storm that could cause damage to your house.

If N4L discovers a threat that could impact your school we'll reach out with mitigation advice.

Our Security Team
Like a friendly neighbour, our team keeps an eye on your digital infrastructure.

Our security experts will let you know if they see a risk or threat to your network that you need to be aware of.

Incident
This is like an intruder or break-in on your property - an incident has occurred. Our team will help support you with the incident response.

Our security experts will help identify phishing, email compromises and malware incidents at your school.

Exposed Service
An open window is like a misconfiguration that leaves a school at risk. This is not a vulnerability but rather an issue of best practice.

We'll help with improvements to network configuration, system firewall rules and email configuration.

Vulnerability
Like a broken lock on your door, a vulnerability is something that has an exploitable weak spot.

We can help identify vulnerabilities and work with you to fix them.

Let's work together

While we're here to provide support, **it's super important that schools and kura also have broader security measures in place**. That's why we've teamed up with the Ministry of Education to help you understand what you can do to improve your school's cybersecurity posture and better protect against online threats. Let's all work together to help keep each other safe.

Support through expertise, tools & insights

Whether it's a quick query or a tricky technical one, we have the right support ready to help your school or kura. You can choose how you'd like to access information and assistance - it's all about what works best for you.

MyN4L: More visibility. More control.

MyN4L is our self-service platform that gives you more visibility and more control over your school's online environment.

It features smart and simple tools that build on services your school already uses to show what's happening on your network and make changes in a few clicks.

You can use MyN4L to:

+ View quarantined emails and safely release any legitimate ones.
+ See what websites are being accessed and blocked on your school's network.
+ Manage access to your school's Wi-Fi network for different types of visitors.
+ Easily add and remove third-party devices from your Wi-Fi network, such as printers and CCTV.

+ Get visibility of the performance of your Wi-Fi network equipment, helping diagnose issues.
+ Request to block and unblock websites according to the needs of your school.

Support Hub

Find a huge range of resources from FAQs to support articles and training guides. Chances are, the answer to your question is on Support Hub at n4l.co.nz/support.

School Relationship Managers

Your dedicated local point of contact gets to know your school, keeps you up to date and provides support when you need it.
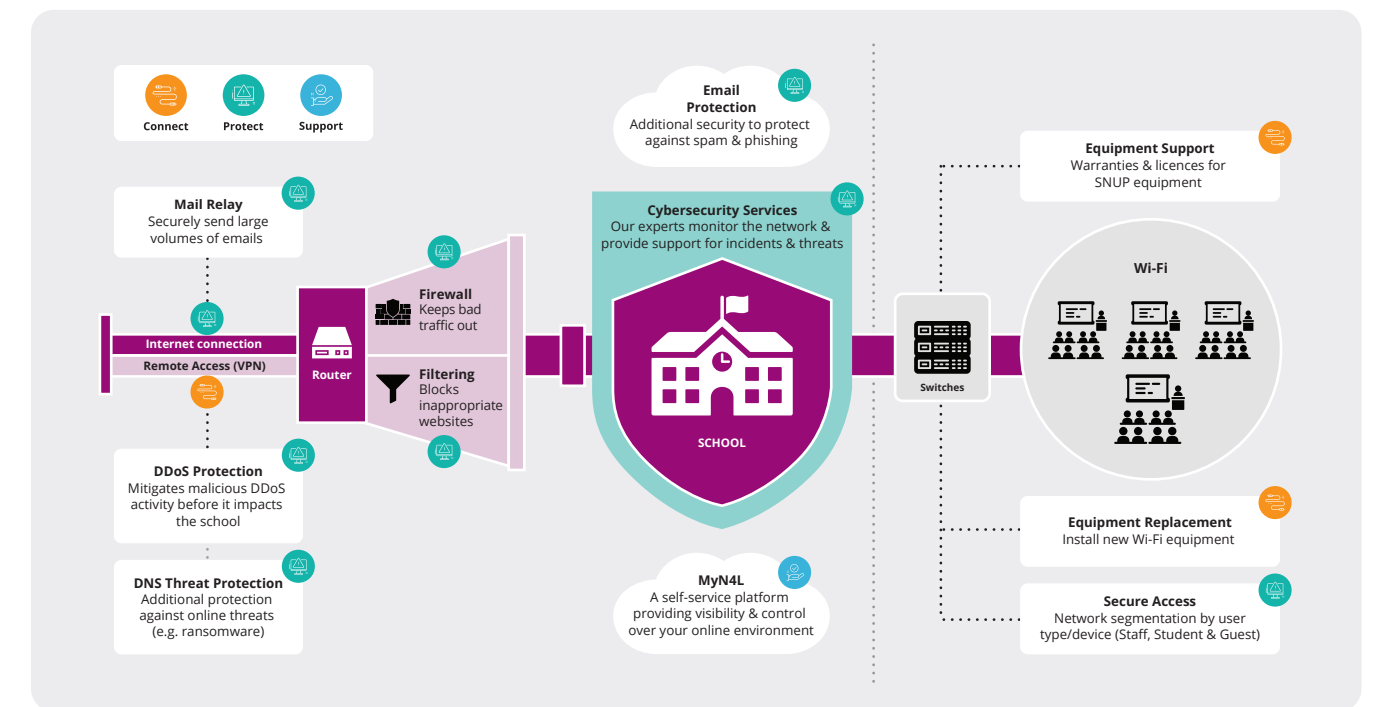
Customer Support team

Our dedicated team is just a call or email away, ready to assist or connect you with the right type of help.

The Managed Network

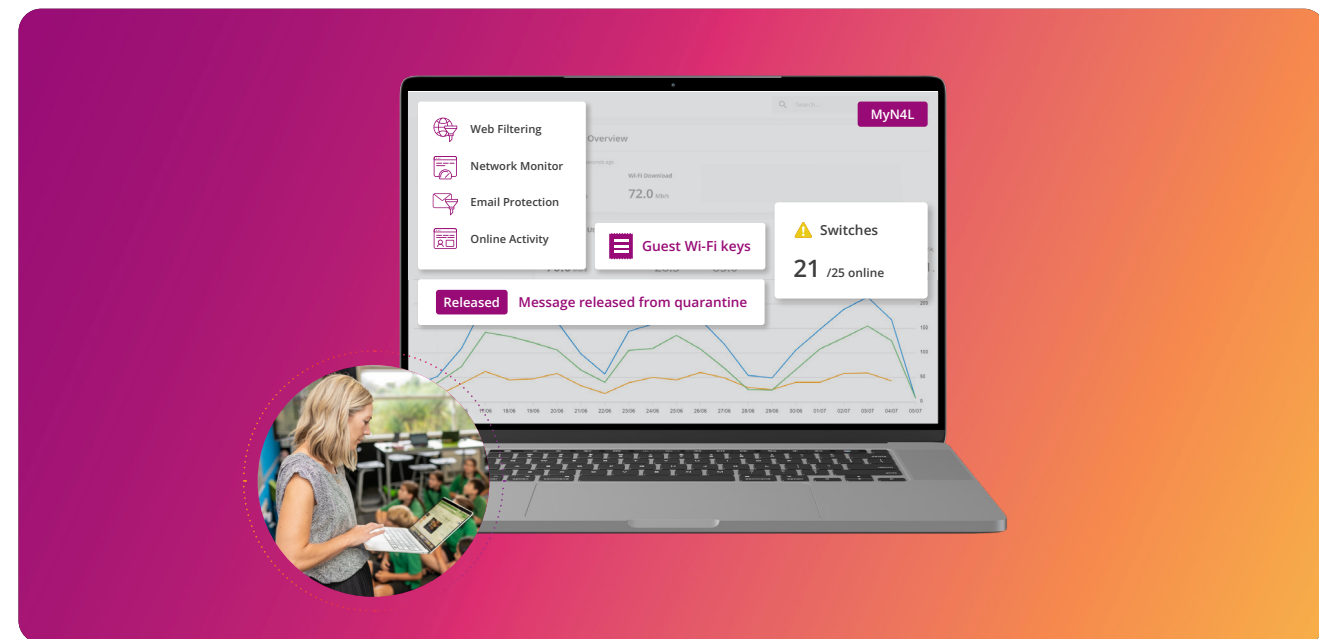**Ever wondered how all of our products and services fit together? This infographic helps to explain.**

Key highlights

Users on the network	Daily business internet traffic	Connect	Customer satisfaction
905 THOUSAND	**25%** SHARE	**2,500+**	**92%**
Making us one of the largest broadband networks in Aotearoa.	Our Managed Network is responsible for nearly 25% of the country's daytime business internet traffic.	More than 2,470 schools and kura in Aotearoa are connected to our Managed Network.	We've maintained our 90% customer satisfaction with schools and kura since launch.

Get in touch

Call the team on **0800 LEARNING (0800 532 764)** or email **support@n4l.co.nz**