What Secure Access means for your school

Secure Access improves your school's Wi-Fi security by segmenting students, staff, and guests into user groups with separate network and web filtering configurations. Migrating to Secure Access keeps your staff and student data better protected, limits the potential impact of cyber attacks, and gives you more control over the web content each group can access.

The way you enrol devices will be different under Secure Access. Below is an overview on what to expect after Secure Access has been implemented, and some tips and pointers to smooth the transition.

	After Secure Access	Tips and tricks
Enrolling devices on your network	All devices including BYODs and third-party devices need to be enrolled to the new network. This is the key objective of migration day. Every device connected to your Wi-Fi network has a unique login. This makes it much easier to know who is using your network and detect when a device is infected with malware.	We suggest using a Mobile Device Management (MDM) system to manage your devices. We recommend building device enrolment into your back-to-school programmes to ensure all staff, students, and their devices have access to the network as the school year commences. As new ākonga and team members join you throughout the year their devices need to be enrolled as well. Add this task to your orientation or onboarding checklists. Your IT support or IT provider should also keep track of when the enrolment of a device expires (typically after 3 years), and when a device is replaced because these devices will need to be re-enrolled.
Logging in to the network	Once a device is known to the network it remembers login details, so users don't need to log in every time they connect.	If a device experiences issues logging in after migration it's likely that the device wasn't properly enrolled. We've prepared some handy guides to help you troubleshoot log in glitches. The classic 'switch the device on and off' trick often resolves any connection issues.
Casting content	Casting devices in your school are enrolled on the Staff network. This means kaiako can find, wake and share directly from any casting device.	Available casting devices may not show on student devices, as they are on a different network. Teachers who want to share content from student devices via casting can do so using existing school collaboration tools, such as Google Meet, Microsoft Teams or Zoom.

Printers	Wireless printers at your school are now connected to a new network. This means you can control which guests have access to printing. The set-up for your wired printers remains the same.	Our printing troubleshooting guide can help you identify and resolve printer issues. Check in with your IT support or IT provider before calling your printer's vendor (note if you involve your IT provider any associated cost would need to be covered by your school).
Ākonga (students)	Every student has unique login details which makes it easier to identify when a device is infected, and to monitor any attempted access of inappropriate content.	Ākonga can use their existing Google or Microsoft 365 credentials to enrol into the new network. Shared devices don't require an individual login. If a class of 30 ākonga share 20 devices, those devices won't have a unique identity to track security issues or attempted access of inappropriate content.
Kaimahi (staff)	Because they're now on a separate network, staff can have access to internet content that may be blocked for students, such as social media. Your team's school-owned devices and personal/BYOD devices are now on different networks, with different types of access. School staff who deal with guests use MyN4L, our self-service platform, to manage guest Wi-Fi access.	Make sure your team members connect their different devices to the right networks. Ensure that your team has been trained on the benefits of Secure Access and how it changes their use of devices, especially when they log on to casting devices and printers. Our Training Hub has been created together with UTB to provide you with a variety of educational materials to help boost confidence and support school staff with your Secure Access network. If you are the school principal, make sure you've logged into MyN4L, our self-service platform, and given user permissions to the members of your team who sort out network access for guests and manage devices. Additional info about how to use the guest access tool in MyN4L can be found here.
Guests	Guests have a separate network with a single Wi-Fi key. To help protect your network, this key automatically resets every month. Guest Wi-Fi access is managed using the Guest Access Limited tool in MyN4L, our self-service platform.	Guests must enter the updated Wi-Fi key each month to access the school's Wi-Fi if their visit extends beyond that period. The monthly Wi-Fi key can be reset at any point in time for security reasons. Once reset, the current key will instantly expire and the new key will be emailed to all nominated school staff contacts, with its expiry time the same as the original key. Guest Access Plus, available via MyN4L, allows your guests to have casting (where compatible) and printing permissions. This flyer has an overview of the various Guest Access options.
Professional Learning and Development facilitators	PLDs can automatically connect to your network when they arrive on site. PLDs will have ready access to casting (where compatible) and printing.	A new solution for the Ministry of Education registered PLDs who work across a number of schools. A QR code can be displayed at your reception area for those PLDs who haven't enrolled their devices yet, or they can use Guest Access Plus until they're set up on the system. PLDs can cast, although not all casting devices might be compatible. For more information see these FAQs.

Where to find more information

There's plenty of Secure Access resources which you may find useful, including our Training Hub, which is full of educational materials to boost confidence and competence of school staff with your Secure Access network.

Following the migration you can contact our friendly Customer Support team on **0800 LEARNING** if you experience any issues with your devices or network. If required, we'll contact your assigned IT partner within their 30-business day warranty support period to arrange remediation.