Cyber safety and web filtering

What you need to know when it comes to online safety and web filtering

When it comes to online safety, we understand how important it is for you to feel confident that you have the right measures in place to protect ākonga while at school. This requires a multi-pronged approach with several elements to consider.

One part is content filtering which can help prevent ākonga from accessing inappropriate or distracting content, based on a school's settings. However, there are several solutions available and we know tech can be complicated. To help you with this and make active choices to keep ākonga safer online, we've included a checklist below. Plus, over the page you'll find a guide on the different roles we all play. This may be especially helpful for those in leadership roles or on school boards.

Ask N4L about...

- [ ] If you've opted-in for N4L's fully-funded Safe & Secure Web Filtering and DNS Threat Protection - it's up to each school to decide which settings best suit their environment. DNS Threat Protection provides an additional layer of protection against unwanted content and also enables SafeSearch for Google and Bing.
- [ ] Reviewing the Web Filtering categories that are blocked and whether these need to be updated - there are 17 categories we recommend schools block as part of our Safe & Secure Internet recommended settings. You can choose to block additional categories, e.g. social media, and a complete list is here. Also review if there are specific websites or applications that should be blocked.

For support with the above, call us on **0800 LEARNING (0800 532 764)** or email support@n4l.co.nz.

Speak with your internal IT lead or IT provider about...

- [ ] If you have N4L's DNS Threat Protection enabled, ensure that your school's DNS is set to the correct DNS server otherwise you won't be benefiting from this protection.
- [ ] Review and update any appropriate Google or Microsoft settings (N4L doesn't have visibility of a school's settings for these platforms).
- [ ] If using Google Workspace for Education, check you have appropriate YouTube permissions in place to help filter video content. Note, YouTube's Restricted Mode heavily relies on users flagging inappropriate content.
- [ ] Google Classroom users can block YouTube for students so they can't search for content but they can access teacher approved content from within Google Classroom.
- [ ] Some schools may also use other third-party providers for web filtering services, so it's worthwhile reviewing these settings as well.

We also recommend...

- [ ] Ensuring appropriate policies and user agreements are in place. Netsafe's Kete has a range of online safety resources for schools and kura.
- [ ] Taking a look at the Ministry of Education's Digital technology: safe and responsible use in schools guide and their Google Workspace Health Check resources.

When it comes to online safety, we all have a role to play

Whilst not all-encompassing, below is a useful guide for principals and school board members.

Board

Ensure policies are in place to protect the online safety and wellbeing of the school, teachers, students and whānau.

Things to consider:

- Have appropriate policies and procedures in place.
- Establish an online safety posture for your school.
- Conduct an annual review of online safety and security settings (e.g. N4L's Safe & Secure Internet service, Google Workspace) to ensure they satisfy the school's requirements.

School Leadership Team

Lead the strategic implementation and day-to-day decision making regarding online safety and student wellbeing.

Things to consider:

- Develop a safe-use strategy to help deliver the school's online safety posture.
- Work with the IT contact to conduct a termly review of settings (N4L's Safe & Secure Internet service, Google Workspace, online safety measures such as YouTube Restricted Mode, etc.) to ensure they satisfy the school's requirements.
- Ensure user agreements are in place.
- Provide PLD for staff to raise awareness of and promote positive digital citizenship (check out Netsafe's Capability Review Tool).
- Raise awareness of online safety in the community.

IT staff or partners

Day-to-day management of the school's online safety and security measures, and managing any changes to settings.

Things to consider:

- Work with N4L to ensure the online safety decisions made by School Leadership are in place.
- Manage settings by other providers such as Google Microsoft, YouTube or third party filtering solutions.
- Consider if there are other suitable solutions that could be implemented, such as SSL Inspection.
- Provide guidance to ensure any services, software or devices interacting with a school's network are implemented safely and securely.

**Note, responsibilities for IT providers are governed by the terms of a school's individual agreement.*

N4L

Provide schools access to fully funded online safety and security solutions, such as Web Filtering, Firewall and DNS Threat Protection. It's up to the school to tell us whether they want these services enabled and the filtering categories, websites or apps they want blocked. We have recommended settings, which are applied based on the school's request and remain as is unless we're asked to make a change.

How we help:

- Ensure N4L services and settings are applied as requested.
- Monitor the status of Safe & Secure Internet services and the applicable recommended settings, and notify the school if any of these become non-compliant.
- Provide guidance to help schools configure the network to meet their online safety needs.

N4L's Safe & Secure Internet

Our Safe & Secure Internet service is designed to provide a baseline level of protection and includes Web Filtering that helps block inappropriate websites and apps, as well as DNS Threat Protection which also enables SafeSearch. N4L's Web Filtering blocks websites and URLs, but not specific content within a website. For example, YouTube is widely used to support learning - schools can currently either allow YouTube, or block all access to it. It cannot filter out individual YouTube videos.

An important note on VPNs and mobile data

Virtual Private Networks aren't all bad, but they can be used to bypass a school's filtering. Please also note our Web Filtering works when a device is connected to the school's network - we have no control when a user is on mobile data. That's why it's important to remember there's no way to guarantee 100% protection for inappropriate content. There are other actions schools can take, like promoting digital citizenship, and making sure policies and user agreements are in place. Check out Netsafe's Kete for useful resources.

Our Customer Support team is always here to help review or change your school's Safe & Secure Internet settings, including the web filtering categories. If you don't have an IT provider, we can put you in touch with our IT panel members in your area. Call us on **0800 LEARNING (0800 532 764)** or email support@n4l.co.nz.