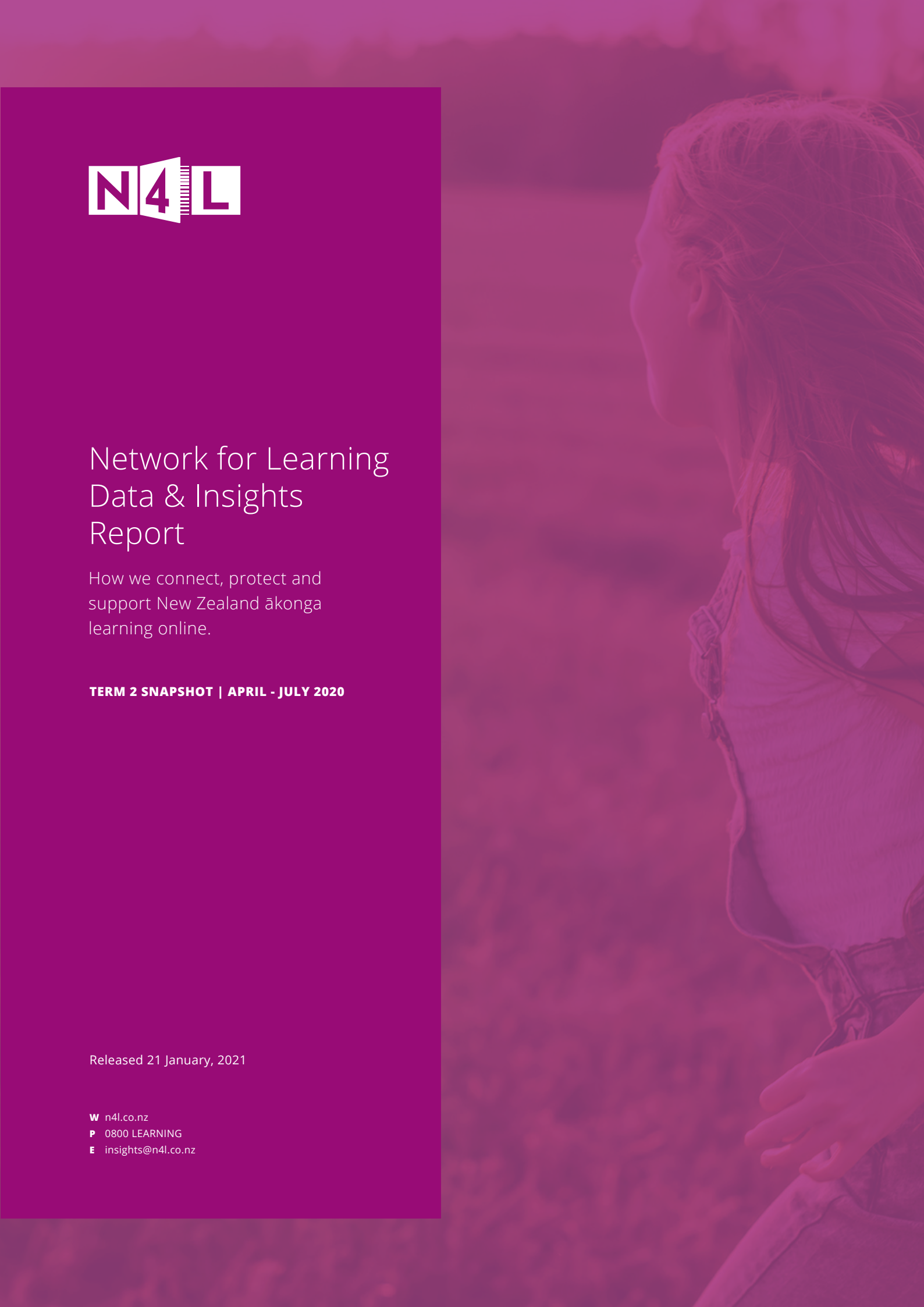


Network for Learning Data & Insights Report

How we connect, protect and support New Zealand ākonga learning online.

TERM 2 SNAPSHOT | APRIL - JULY 2020

Released 21 January, 2021

W n4l.co.nz
P 0800 LEARNING
E insights@n4l.co.nz

Contents

About the report

Introduction

Network for Learning's (N4L) first data and insights report shows New Zealand schools face ever increasing threats to online safety and security.

It also highlights how student data use changes by the size, region and type of school they attend.

With close to 800,000 ākonga (students) and 55,000 educators, N4L operates one of the largest Managed Networks of its kind in the world. Our school internet users consume an average of 174 terabytes (TB) of data per day and use our technology to keep safe from millions of daily online threats and harmful digital content.

This report highlights some of the work we do to connect, protect and support New Zealand ākonga learning online.

It is a massive job involving many partners across government, education and the technology sectors to make it happen. The aim is to share data and insights with these partners and the growing network of organisations and decision-makers serving our school communities.

We welcome your feedback! Please email us at insights@n4l.co.nz if you would like to send input to the team and receive a notification of when our next report is published.

Report dates

We focus on the second school term, April 15th - July 3rd 2020, which included 22 weekdays when schools were closed due to the COVID-19 nationwide lockdown. During this time, students were learning from home and not using our network. Throughout the report, some comparisons have been made to the data from the previous term (January 27th - March 27th), when schools were closed for up to four days.

About the data

All information in this report is aggregated and no school or individual can be identified. You can find out more about how N4L collects and uses data from the Managed Network in our Privacy Statement. An independent third party assisted with the data work in this report (Datamine Limited).

N4L's Managed Network internet services are used by all state and state-integrated schools. When school internet users visit and search for websites, the amount of data consumed, and where it stems from (website domains), is collected in accordance with our Privacy Statement. The data consumption includes automated traffic such as software updates.

When attempts are made to visit websites that our technology has blocked for safety and security reasons, or if a cyber criminal tries to infiltrate the network, these attempts are blocked and recorded through either our Web Filtering, Firewall or DNS Threat Protection services.

It should be noted that visiting a single website can trigger multiple data requests through a school's connection. For example, a banner advert or a third party widget embedded in a website can send requests to other websites without the user clicking on these links.

Term 2 Highlights

Cyber security threats continue to rise.

N4L blocked an average of 2.9 million threats every day across our network when students were at school. Phishing scams continued to dominate the online threat landscape, closely followed by malware and unauthorised attempts to access school systems. A spike in Distributed Denial of Service (DDoS) attacks was noted during the week of May 24th, when students were back at school.

Harmful digital content represents a small proportion of all blocked websites.

Websites considered unsafe for students make up 6% of all blocks made across the Managed Network. Pornography represents just 1.4% of all sites blocked, with 93% of these blocks made within secondary schools.

Student data use changes depending on the size and location of their school.

Secondary school students generally use more than twice as much data as primary school students.

Students attending primary schools with smaller roll sizes tend to use more data than more populated primary schools. And students at the largest secondary schools use less data than those with 400 or fewer students.

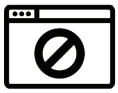
Auckland per-student data use is lower than in other urban centres. The highest regional consumption stems from students attending schools in the West Coast, Manuwatu-Whanganui and Nelson (in that order) with the students in the Marlborough, Northland and Tasman regions consuming the least amount of data.

School internet users spend the most time on websites related to collaborative learning or administering education.

Hāpara's Teacher Dashboard is popular with all New Zealand schools, as are Google-owned websites.

Language-based learning websites feature more prominently than online maths sites.

While 25% of data consumption stems from streaming media sites, neither Netflix nor YouTube feature on the top 10 list of websites where students spend the most time.



Blocked websites keep students focused on learning.

Schools are keeping students focused on learning by choosing to block websites featuring file sharing and storage services, gaming, software downloads and social networking sites. Together these sites represent more than two thirds of all blocked web content.

Connect - data use in schools

N4L connects 2,457 schools to fast, reliable, safe and secure internet for learning. These include:

1,916 primary schools[1], which account for more than 493,000 students across New Zealand.

465 secondary schools, which account for more than 299,000 students across New Zealand.

Term 2 data consumption

Schools consumed 9.9 petabytes of data during Term 2, which ran from April 15 - July 3 2020.

Lockdown impact

Daily student data consumption declined by 9% between Term 1[2] **and Term 2.** This shows the impact of the nationwide lockdown, where students lost 22 days of in-school learning time and were not using their school's internet. Once students returned to school following the end of lockdown, Term 2 daily data consumption increased above the average for Term 1.

When comparing the two terms, we found that while secondary school students used 14% less data per day in Term 2, primary school student data consumption increased by 3% per day.

Further insights:

- **Secondary school students** consumed more than twice as much data per day than primary school students, using an average of 242 Megabytes (MB) each day, whereas primary students consumed 98 MB.
- **Students in the smallest secondary schools**[3] **use more data** than those in the largest secondary schools. However mid-sized secondary schools generally use more data than either larger or smaller secondary schools.
- **Primary school students** consuming the most data attend schools with 100 or fewer students, whereas data consumption habits are similar for students in mid-size and larger primary schools.

Consumption per student per day

98 MB **3%**

used by the average primary student per day in Term 2, an increase of 3% compared to Term 1, 2020

242 MB **14%**

used by the average secondary student per day in Term 2, an decrease of 14% compared to Term 1, 2020[4]

1. Refer to glossary for a definition of primary and secondary schools.
2. The school term began during Alert Level 4 with students learning from home. Most students returned to school on Monday May 18th, following the move to Alert Level 2 on May 13th at 11.59pm.
3. Refer to glossary for explanation of school roll sizes.
4. Daily consumption increased once students returned to school.

Streaming media data use

Streaming media refers to those websites that contain multimedia files that can be played or downloaded and accounted for 25% of all data use in schools in Term 2. YouTube was the most popular streaming media platform for both primary and secondary schools, but did not feature on the top 10 sites where students spent most of their time. See next section on websites and browsing time.

Social networking data use

In contrast to streaming data, social networking was responsible for just 1.2% of all data consumption; it made up 2% of secondary school data consumption and 0.9% of primary school data consumption. Facebook was the most popular social networking site across primary and secondary schools.

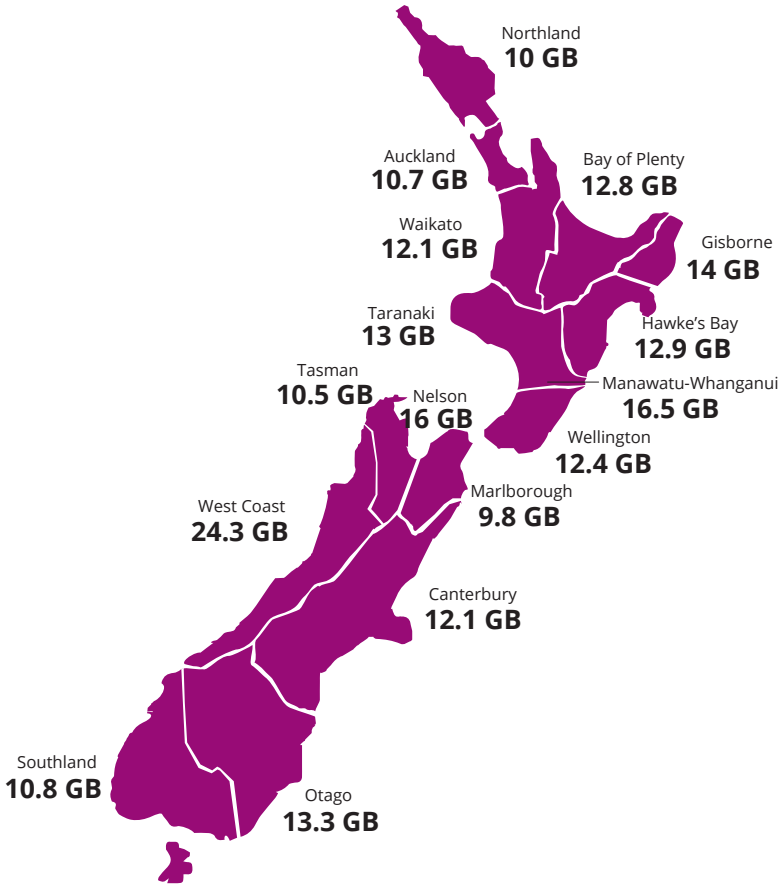
Regional data use

While student data use in rural and urban schools was similar, we noticed some differences across the regions. The graph below shows the distribution of all Term 2 internet traffic in each region across all schools.

Students attending West Coast schools consumed the most data, using twice as much data as the average Auckland student. West Coast schools are smaller, with fewer students in the region. With only 34 schools on the West Coast (representing 0.6% of the total student population), compared with 512 schools in Auckland (representing 33.6% of all students), the difference may be skewed by one or two "outlier" schools that consume a lot more data.

In fact most students outside of Auckland consumed more data than their Auckland counterparts. Students in just three regions consumed less data on average than Auckland in Term 2: Northland, Marlborough and Tasman. The distribution of traffic between secondary and primary schools is illustrated in Appendix 3.

Consumption per student per region in Term 2



Percentage of students in each region

Auckland	**33.6%**
Canterbury	**11.8%**
Wellington	**10.7%**
Waikato	**10.1%**
Bay of Plenty	**7.0%**
Manawatu-Whanganui	**5.2%**
Otago	**4.3%**
Hawke's Bay	**3.9%**
Northland	**3.9%**
Taranaki	**2.7%**
Southland	**2.2%**
Gisborne	**1.2%**
Nelson	**1.1%**
Tasman	**1.0%**
Marlborough	**0.9%**
West Coast	**0.6%**

Source: Statistics NZ

Connect - websites and browsing time

The two tables indicate where school internet users are spending the most time online, and are ranked according to the total browsing time spent on each site. Website sub-domains are grouped under the larger domain names for this analysis; for example, traffic going to edu.google.com is classed as Google traffic. Note this metric (time) does not necessarily indicate that more data was consumed while at each of these sites.

The time spent on each of the listed websites is illustrated in Appendices 4 and 5.

Top 10 websites by browsing time: education category

	Primary (Education)	Secondary (Education)
1	Hāpara Teacher Dashboard	Grammarly
2	Seesaw	Hāpara Teacher Dashboard
3	eTAP	G Suite for Education (Google)
4	Grammarly	school.nz[1]
5	Epic	Education Perfect
6	Prodigy Education	Language Perfect
7	Linc-Ed	Texthelp
8	ClassDojo	Seesaw
9	3P Learning	Kahoot
10	G Suite For Education (Google)	ClassDojo

Top 10 websites by browsing time: all websites

	Primary (All)	Secondary (All)
1	Google	Google
2	Apple	Microsoft
3	Microsoft	Windows
4	Facebook	Apple
5	Hāpara Teacher Dashboard	Facebook
6	Windows	Office 365
7	Linewize	Linewize
8	Office 365	Spotify
9	Seesaw	Adobe
10	Bing	Bing

Education-related websites - These sites range from sharing platforms that allow student classwork to be shared with teachers and parents (Seesaw, ClassDojo, Linc-Ed, Hāpara's Teacher Dashboard), to sites offering online learning activities (Prodigy Education, Kahoot, 3P Learning, Education Perfect), and also include educational reference sites (Grammarly, Texthelp and Epic).

Tools allowing schools to manage student administration (eTAP) and documents (Google Suite for Education) also feature in this category, as do school-owned websites (ending in school.nz).

Maths learning - For primary schools, two of the top 10 websites offer maths learning activities: Prodigy Game and 3P Learning, with the former focusing solely on maths and the latter offering a range of resources in addition to maths, like spelling and literacy. One of the top 10 websites listed for secondary school students includes maths learning activities (Education Perfect), while Kahoot allows users to generate multiple-choice quizzes on any topic, including maths.

Languages - Two of the top 10 websites for primary school students offer language-related resources: Grammarly and 3P Learning. In contrast, half of the top 10 secondary school sites offer language learning resources: Grammarly, Education Perfect, Language Perfect, Texthelp and Kahoot.

All website types - The sites where school internet users spend most of their time offer collaboration suites and platforms to create, share or manage content.

Google, Apple & Microsoft - The world's largest technology companies are listed among the top three websites for primary and secondary schools. Google features most prominently across all schools. Primary school students spend more time on Apple than Microsoft, while the reverse is true for secondary school students. It is worth noting that automated software updates are issued frequently by these three companies, and this contributes to the length of time spent on these sites.

Facebook and Spotify - The time spent on Facebook represents just 1.5% of all time spent online. Many schools use Facebook groups to share information with their parent communities. Spotify hosts music and podcasts that can be used to aid learning.

[1] Websites ending in school.nz.

Protect – cyber security (blocking online threats)

Security blocks: N4L mitigates the impact of cyber threats, such as phishing scams, ransomware, command and control servers (linked to malware), DDoS (Distributed Denial of Service) attacks[4], and stops unauthorised attempts to access school data. Malicious actors continue to find new vulnerabilities to exploit.

The rise of security blocks in Term 2

In Term 2, N4L blocked more than

120 million cyber security threats

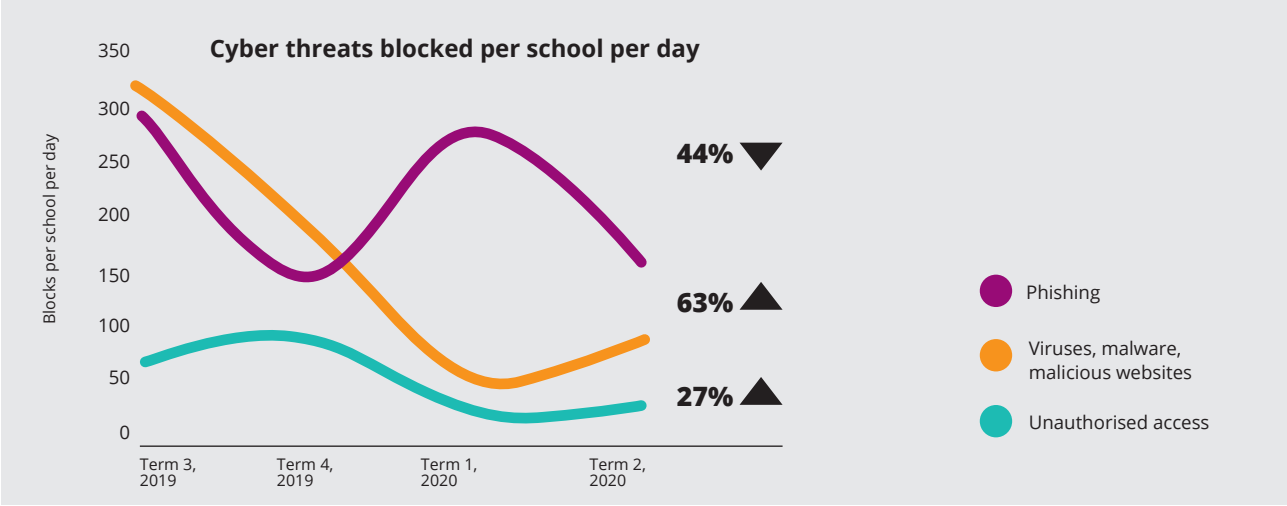
an increase of 13.7% since Term 1.

The 13.7% increase occurred despite the nationwide lockdown translating to fewer days at school. N4L's technology blocked an average of 1.9 million security threats each day in Term 2, compared with 2.2 million per day in Term 1. **However, the average number of blocks rose to 2.9 million per day once lockdown lifted and students returned to school, leading to the 13.7% rise in Term 2.**

While **phishing threats** were the most commonly blocked cyber threat, with 152 blocked at each school every day over all of Term 2, the number of phishing threats blocked per school, per day declined by 44% compared with Term 1.

At the same time, the number of blocks made against **viruses**, **malware** or other malicious websites targeting school networks increased by 63% per day, per school. Blocks against unauthorised attempts to access school networks increased by 27%.

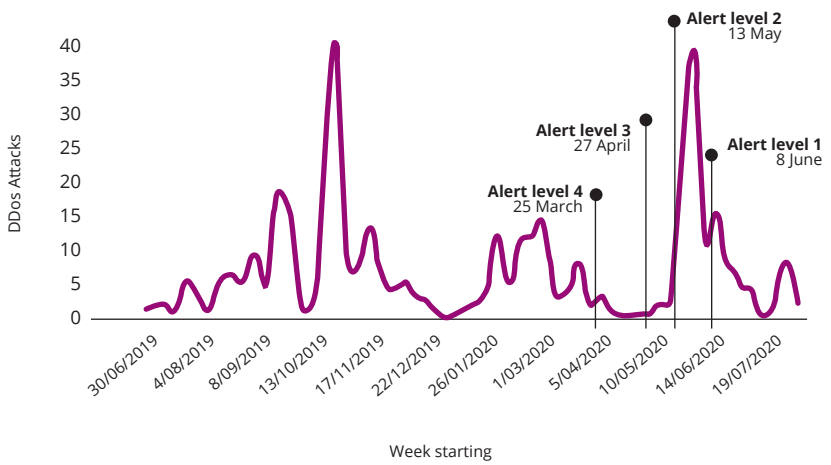
There are many other types of security threats that N4L blocks, including **DDoS attacks**. The graph below charts only the most commonly blocked threats. Examples of other security blocks include command and control blocks, where attackers send commands to systems compromised by malware in an attempt to steal information.



Distributed Denial of Service (DDoS) attacks

increased by 45%

in Term 2 compared with Term 1, with a spike occurring the week of May 24th, which is the week after students returned to school following the nationwide lockdown.



[4] Refer to glossary for explanation

Protect – cyber safety (blocking harmful digital content) & other website blocks

Safety blocks: Websites hosting harmful digital content such as pornography or graphic violent images are blocked by N4L's filtering by default.

There were 91 million safety blocks in Term 2 (or 1.5 million per school day), up 0.7% from Term 1. Safety blocks make up 6% of all blocks made across the Managed Network.

All blocked categories - 1.5 billion (or 24 million blocked per school day)

In addition to the default categories blocked by N4L, schools also use our filtering to block content they deem inappropriate for learning or distracting for students, such as social media or gaming sites. Not all schools will have the same websites blocked. The combination of safety blocks and additional websites blocked by schools are referred to as 'website blocks'.

The number of website blocks increased by 15% in primary schools and by 40% for secondary schools compared with the previous school term.

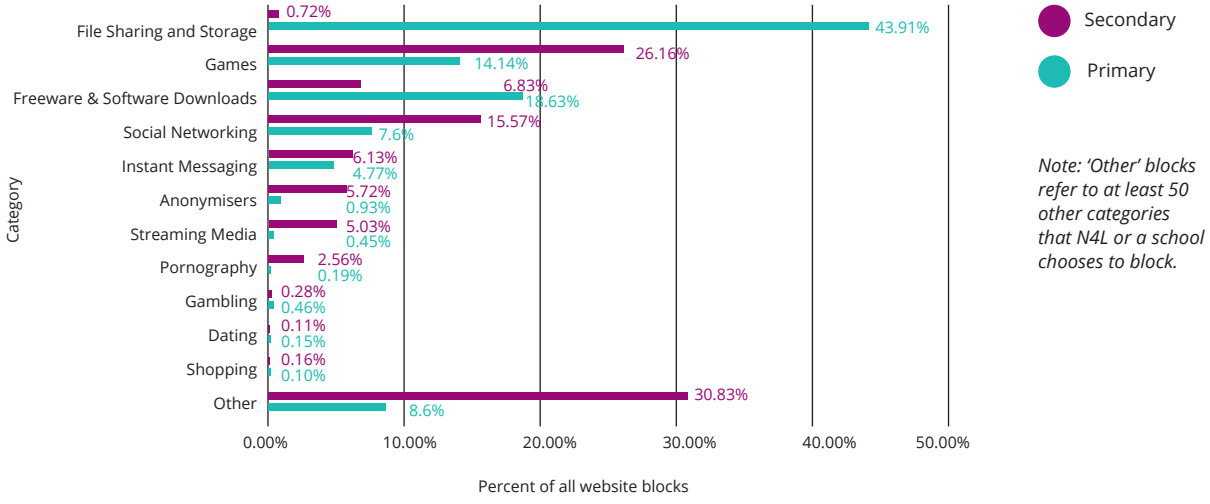
91 million .7%

Safety blocks in Term 2, 2020, a 0.7% increase on Term 1, 2020.

1.5 billion 22.4%

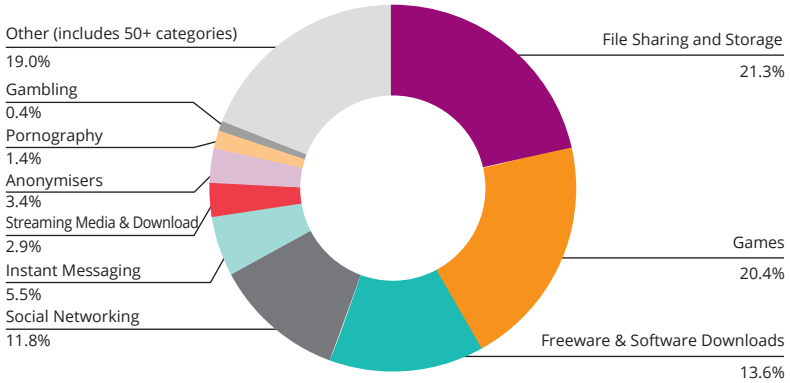
Websites blocked in Term 2, 2020, a 22.4% increase on Term 1, 2020.

Commonly blocked categories (Graph 1)



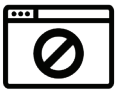
Note: 'Other' blocks refer to at least 50 other categories that N4L or a school chooses to block.

Commonly blocked categories as a percentage of all website blocks (Graph 2)



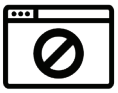
File sharing and storage websites are blocked the most, and comprise 21% of all blocked websites; however the majority of these blocks are made by primary schools (44%). This category includes content hosted on websites like iCloud, Dropbox, or other file storage sites.

Notable changes in website blocks between Terms 1 and 2



Gaming blocks increased 99% in primary schools in Term 2 versus Term 1; and rose 24% in secondary schools. They represent 20.4% of all blocks made, with over twice as many gaming blocks made at secondary schools compared with primary schools. (Refer to Graph 1).

Pornography blocks decreased by 42% in secondary schools in Term 2, yet increased by the same amount in primary schools. The category represents 1.4% of all website blocks for both secondary and primary schools, with 93% of pornography blocks made at secondary schools. Graph 1 (on the previous page) shows that 2.6% of all secondary school website blocks are related to pornography whereas just 0.2% of all primary school website blocks relate to this category.



Anonymiser blocks[5] **increased by 34% overall in Term 2**. Anonymisers can be used to defeat filters and the bulk of these are made at secondary schools (88%). While these blocks occur at school, it is interesting to note that anonymiser blocks also feature prominently in a new N4L 'Switch on Safety' filter parents can use to block unsafe websites from home (refer to Appendix 2).

[5] Refer to glossary for explanation

Support - for schools and their technology providers

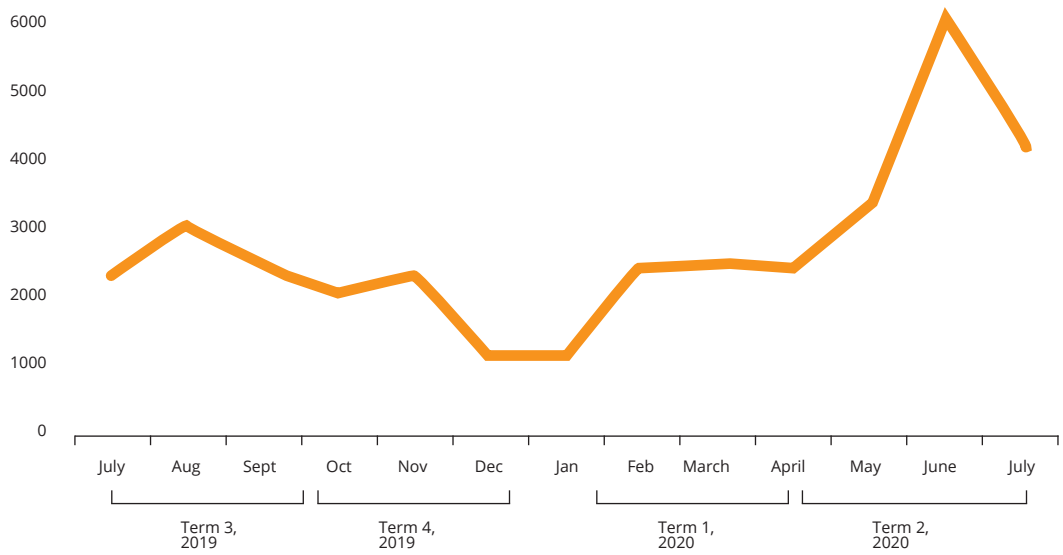
The N4L Helpdesk team ensures schools have access to the support they need, with schools able to log cases via the online Support Hub or by calling the Helpdesk.

The people contacting N4L's Helpdesk range from teaching principals with little or no tech knowledge, to technology companies calling on behalf of the schools they are engaged to support. The latter group represents around 40% of all Helpdesk callers.

As schools returned to full capacity from May 18th, 2020 Helpdesk calls peaked, leading to a 118% increase in cases opened in Term 2 compared with Term 1.

The graph below shows the number of N4L Helpdesk support cases opened per month.

Number of support cases opened per month



95% Term 1, 2020 **95%** Term 2, 2020

Of schools on the network are **satisfied with support** and this was consistent for Term 1 and Term 2, 2020.

90% Term 1, 2020 **88%** Term 2, 2020

Of support calls are **answered within 30 seconds.**

53% Term 1, 2020 **28%** Term 2, 2020

Of calls are 'service requests', for example, when a school is configuring new hardware they've purchased.

7% Term 1, 2020 **4%** Term 2, 2020

Fewer than 10% of calls are related to incidents impacting the network for that school.

Glossary

Anonymisers	Anonymiser services, such as VPNs (virtual private networks) can be used to defeat filters, allowing internet users to browse websites that may otherwise be blocked by N4L's filtering.
Command and control server attack	Computers controlled by attackers are used to send commands to systems compromised by malware; this computer is called the command & control server. This enables attackers to receive stolen data from targeted networks.
Distributed Denial of Service (DDoS)	A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal internet traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.
Primary and secondary	In this report, primary schools include years 0-8 and secondary schools include years 9-13. Intermediate schools (years 7&8) are grouped with primary schools. However, some secondary schools include years 7&8 and this data is included in the secondary school findings. Composite schools, which offer a range of years from 0-12, are grouped with the secondary school findings.
Safety blocks	N4L blocks websites that are unsafe to students and includes content like pornography and graphic violence. These are called safety blocks. ***The list of safety block categories includes:*** Alcohol, Child Abuse, Dating, Discrimination, Drug Abuse, Explicit Violence, Extremist Groups, Gambling, Hacking, Illegal or Unethical, Lingerie and Swimsuit, Marijuana, Nudity and Risque, Other Adult Materials, Plagiarism, Pornography, Proxy Avoidance , Tobacco, Weapons (Sales)
School rolls	Secondary schools generally have larger school rolls than primary schools. The average secondary school has 646 students, while the average primary school has 257 students.
Security blocks	N4L mitigates the impact of cyber threats, such as phishing scams, command and control servers, DDoS attacks; and stops unauthorised attempts to access school data. ***Included under security blocks:*** Malware, Unauthorised access attempts, Phishing attempts, Viruses, Command and control servers, DNS exfiltration, Dynamic DNS, Malicious websites, Newly observed domains Newly registered domains, Spam URLs
Website blocks	The total number of all websites blocked by N4L's filtering. This includes both safety blocks, which are explained above in this glossary, as well as websites blocked optionally by schools, such as games or social media. Not all schools will have the same websites blocked; it depends on the school's choice.

Appendix 1

Appendix 1

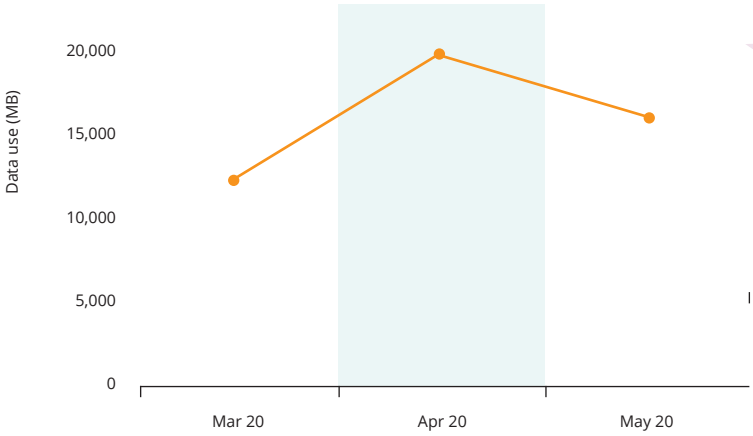
Digital inclusion - connecting students from home

N4L has extended the use of its Managed Network services into the home for some students living without access to reliable internet beyond the school gate.

The company has been piloting ways for ākonga to learn from home, with their whānau. N4L is working alongside the Ministry of Education, technology companies and community organisations to trial different ways to provide safe (filtered) connectivity.

In Term 1 of 2020, the first trial using portable hotspots to provide internet at home began at Te Akau ki Pāpāmoa School and was extended into Term 2. The lockdown emphasised the importance of equitable digital access, with data-consumption-by-user-traffic peaking during Alert Level 4.

Figure 1 - Average data consumption per connected student (MB). Students connected to the 4G pilot used on average between 12-20 GB data per month, with N4L actively managing the wireless broadband connections via its centralised firewall to limit non-educational use.



45MB-98GB

Data consumption varies by user with some using just 45MB (about two minutes of a Zoom call) while others clock up 98GB of data use.

44GB on Zoom

One of the most popular applications of the lockdown was Zoom, with 44GB total consumed as ākonga logged in to online lessons. This aligns with worldwide trends regarding Zoom use.

Visit n4l.co.nz/digital-inclusion to watch the video to this pilot.

"Our families have been so grateful for having the access. They feel a part of the community, and it's brought them into the school. Covid-19 acted as a real-life catalyst, bringing to light that equitable digital access is key to the ability to deliver education from home."

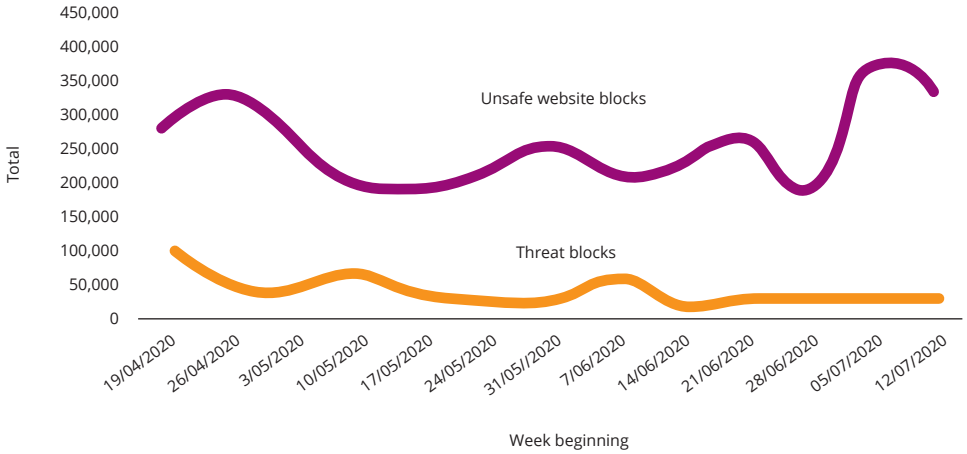
Bruce Jepsen,
Principal, Te Akau ki Pāpāmoa School

Appendix 2

Online safety filter - protecting students from home

Switch on Safety is a filter that parents can set up on their children's learning device to block the worst of the web. It is designed to make the internet safer for all students learning from home and is part of N4L's commitment to provide safer connectivity for learning while students are away from school. The graph below charts Switch on Safety blocks across Term 2 and the school holidays following its introduction for the first day of Term 2, Wednesday April 15th. By the end of Term 2, 25,028 households had downloaded the home filter to one or more of their child's devices. During this time the filter blocked 2.8 million unsafe websites and just under 500,000 online threats.

Figure 2 - Weekly Switch on Safety blocks over time



switch on safety

Blocked websites include those featuring pornography, gambling, cyber-bullying, plagiarism, self-harm and drug and alcohol content.

Websites associated with viruses, malware and scams, and anonymiser services, which can be used to defeat filters, are also blocked, along with other malicious software designed to infect devices and steal information.

Unlike the filtering at school, users can't add sites they want to block. However, N4L's filtering technology adds new unsafe websites automatically as they arise. You can find the full list of blocked categories at switchonsafety.co.nz

Top 10 blocked categories by Switch on Safety filter

576,872	**peer to peer**
322,474	**anonymisers**
97,367	**gambling**
68,563	**pornography**
50,174	**mature content**
18,946	**alcohol**
17,770	**plagiarism**
12,246	**personals and dating**
1,348	**hacking**
1,209	**tobacco**

Appendix 3

Data use: a closer look across the regions

Figure 3 - The distribution of all internet traffic in each region across primary and secondary schools.

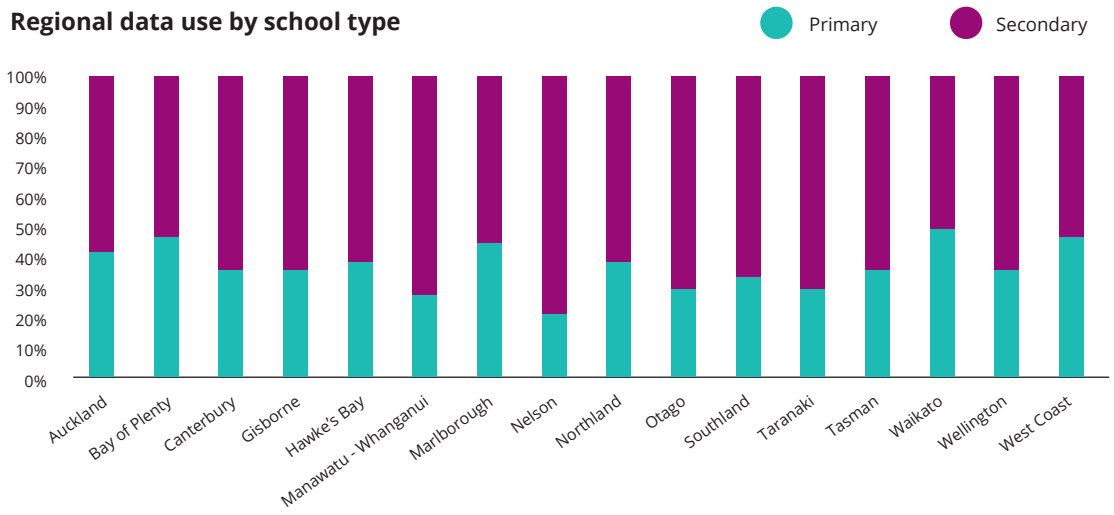


Figure 4 - Percentage change in data use between Term 1 and Term 2 by region.

Regional data use: how much more or less data was consumed in Term 2, compared with Term 1, by primary and secondary schools.

Appendix 4

Data use: browsing time on websites - primary schools

Figure 5 - Where primary school users spend their time on educational websites.

Time spent on educational websites in primary schools

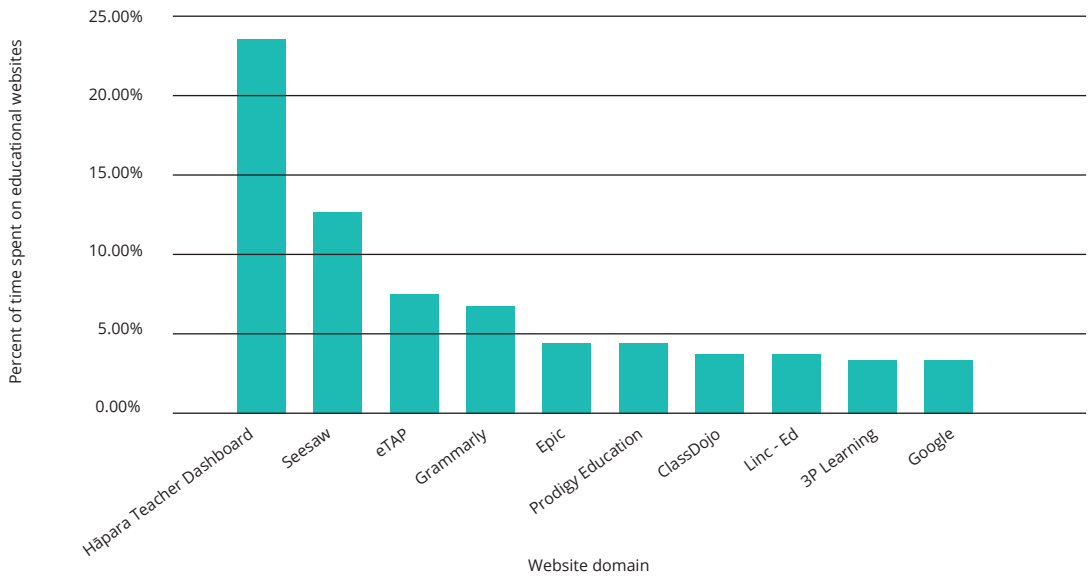
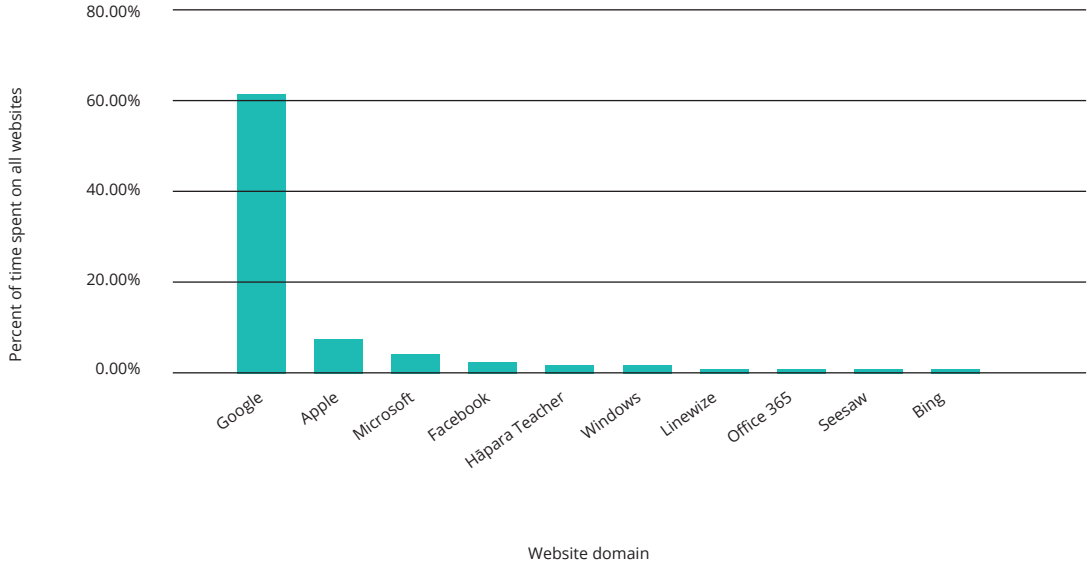


Figure 6 - Where primary school users spend their time across all websites.

Time spent on websites in primary schools



Appendix 5

Data use: browsing time on websites - secondary schools

Figure 7 - Where secondary school users spend their time on educational websites.

Time spent on educational websites in secondary schools

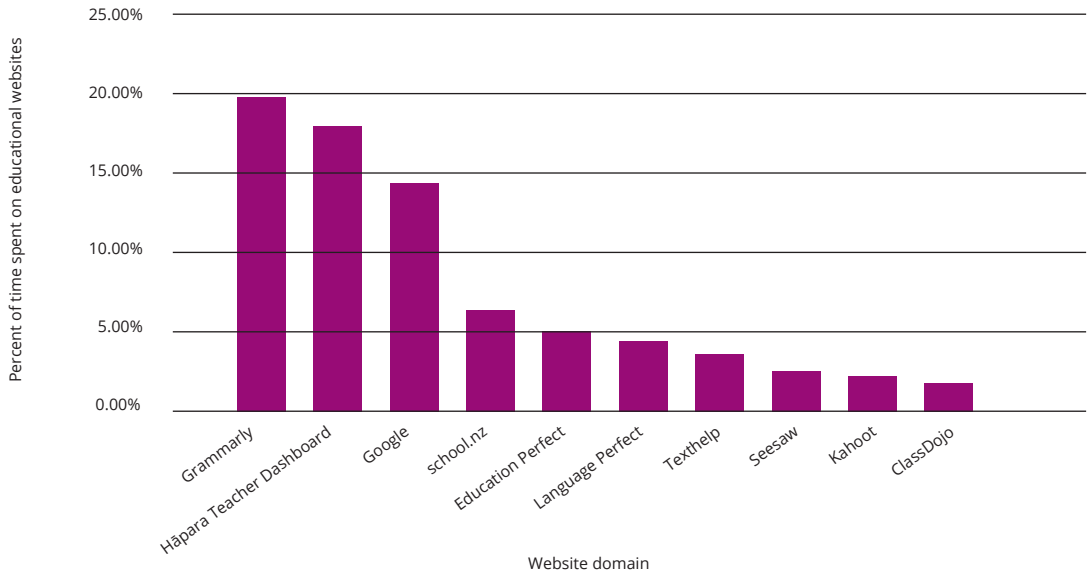
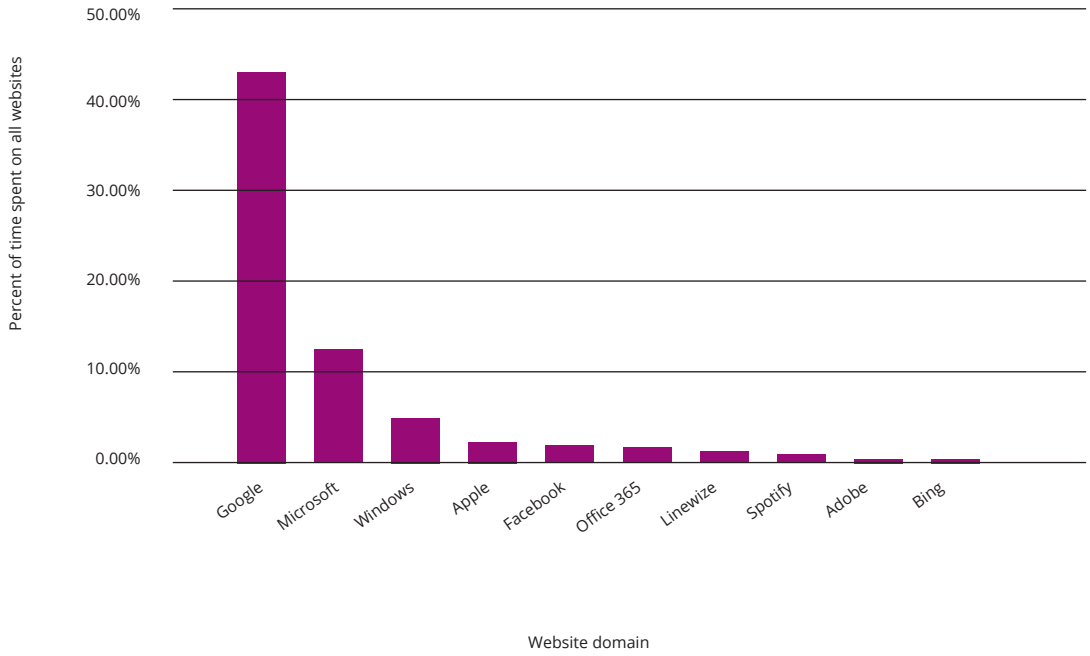


Figure 8 - Where secondary school users spend their time across all websites.

Time spent on websites in secondary schools



Appendix 6

Protecting schools: safety and security blocks

Figure 9 - Daily security blocks per term.

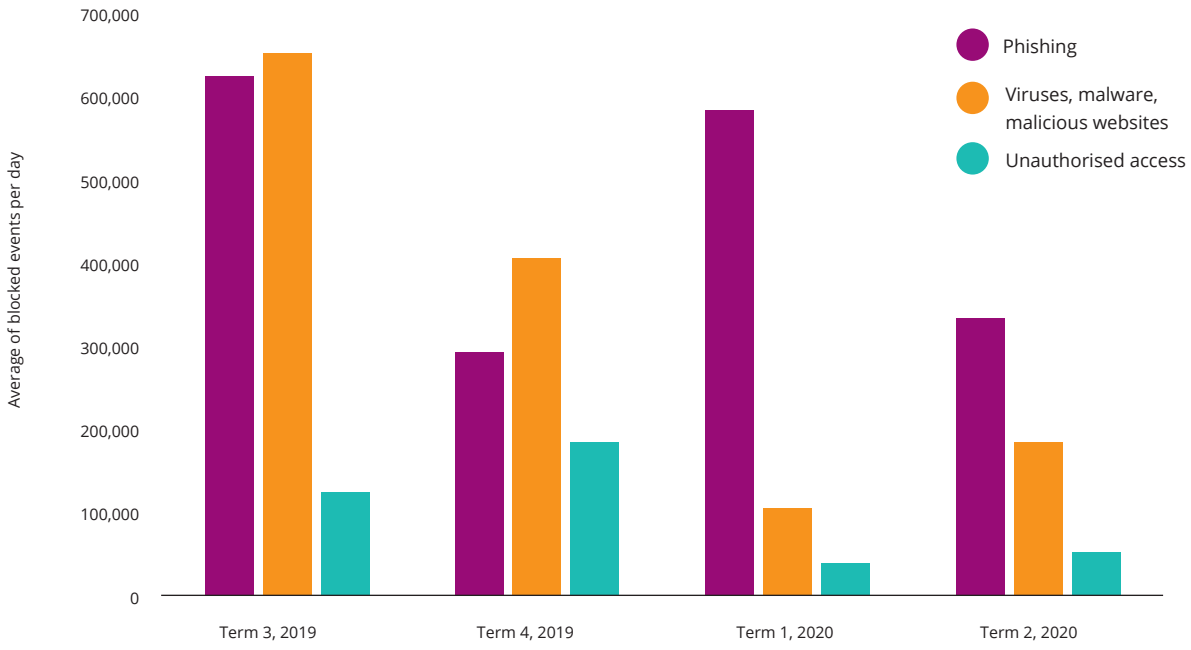


Figure 10 - The percentage change in blocked categories between Term 1 and 2.