

A photograph of a woman with long dark hair, smiling and showing a green smartphone to two young children. The children are looking at the phone with interest. The woman is wearing a dark top. The children are wearing light-colored clothing. The background is slightly blurred, showing an indoor setting with orange curtains. A large teal and blue graphic shape frames the left and bottom of the image.

Annual Report 2022/2023





Content

<u>From the Chair and Chief Executive</u>	1
<u>Year at a glance</u>	3
<u>Our Impact</u>	5
<u>Harmful Digital Communications Service Team</u>	7
<u>Online Safety Operation Centre</u>	17
<u>Engagement (education, research, marketing)</u>	21
<u>Our Priorities (2024 Outlook)</u>	27
<u>Legislation and Compliance</u>	30
<u>Financial Highlights</u>	31

From the Chair and Chief Executive

Chairman's Overview

In a year marked by unprecedented challenges and opportunities, Netsafe has continued to lead the charge in safeguarding online safety and protecting New Zealanders from harmful digital content.

First and foremost, I would like to extend my heartfelt gratitude to Brent Carey as CEO, and the Senior Leadership Team. Their visionary leadership has been instrumental in steering Netsafe toward excellence, innovation, and unwavering commitment to our mission. Under their guidance, we have achieved remarkable milestones, enhanced our relationships with our contract providers (MoE and MoJ), and been active on the local and global stage advancing the cause of online safety.

I would also like to express my deep appreciation to our dedicated staff. Their tireless efforts, resilience, and adaptability have been critical in navigating the ever-evolving digital landscape. In a world where threats to online safety persist and evolve, our team's unwavering dedication to helping all New Zealanders has been nothing short of exemplary.

One group that deserves special recognition is our customer contact centre staff. They have worked tirelessly under trying conditions, often dealing with emotionally charged situations and complex issues. Their commitment to providing support and guidance to those in need has been a beacon of hope in challenging times.

We owe them our gratitude for their unwavering dedication and compassion.

In the past year, we have made significant strides in improving our technology and services. Our innovative solutions have helped countless individuals and organisations in their times of need. We have also continued to foster partnerships with like-minded organisations, NZ government, and stakeholders to collectively address the critical issue of online safety.

As we look ahead, we remain steadfast in our commitment to champion online safety and combat harmful digital content. Our mission is more vital than ever, and we are excited to continue our journey with your unwavering support.

In closing, I want to thank each and every one of you, our stakeholders, for your trust and support. Together, we will continue to make the digital world a safer place for all New Zealanders.



Colin James
Netsafe Chairman



Chief Executive Officer's Report

This year, Netsafe invested heavily in modernising our services, focusing on incident management, education, and outreach. We conducted nationwide discussions on online safety for New Zealanders, which involved relocating our offices, upgrading our contact centre, organising data, and introducing new educational products and online safety campaigns. We also enhanced support through chat services and implemented innovative harm prevention initiatives.

Internationally, we joined the Minister of Internal Affairs on a trip to Europe to learn from other online safety schemes and shared insights on various topics, including image-based abuse, self-regulation, and dispute resolution best practices. Netsafe actively participated in global forums like the Internet Corporation of Assigned Names and Numbers meeting, the Internet Governance Forum of Taiwan, and the International Symposium on Cyberbullying.

Our commitment to fostering important online safety discussions in New Zealand was evident through initiatives such as bite-sized education modules, safety toolkits, a voluntary Code of Practice for Online Safety and Harms, and dedicated online safety weeks (Netsafety Week and Porn Week). In March, we launched Netsafe Lab, aimed at incubating ideas and running experiments to enhance online safety through data, policy development, and technological solutions. The lab will collaborate with global initiatives and local expertise to minimise harm from local issues.

We established new partnerships, including one with the Ministry of Foreign Affairs and Trade, and strengthened relationships with government agencies, the private sector, and NGOs like the Light Project and ID Care, highlighting the demand for our services.

Our research continued to play a crucial role, shedding light on misinformation. With an election on the horizon and changes in the online safety landscape, we are gearing up to provide NGO and Government contracted online safety services.

As Netsafe enters its 25th anniversary year, we are proud of our accomplishments, yet we remain committed to progress. We have brought back the trans-Tasman Online Safety Conference to New Zealand and are preparing to relaunch our online education offerings, revamp an animated series for primary schools, conduct vital research on social media's impact on young people's self-esteem, and introduce more innovative tech tools in the fight against online scammers. The future holds exciting challenges and opportunities as we continue to serve our local and international communities in this ever-evolving digital landscape.



Brent Carey
Chief Executive Officer



Year at a Glance

2022 JULY

Launched the **Aotearoa New Zealand Code of Practice** for online safety and harms

AUGUST

New SLT appointed boosting Netsafe's customer, legal and advocacy leadership capabilities

SEPTEMBER

Launched our first "digital employee" **Kora – the chatbot** – to respond to the public's questions 24/7

OCTOBER

Downsized to new premises as we were joined by new team members from across the motu and enjoyed the flexibility afforded by participating in the **4 Day Work Week pilot**

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES

INHOPE

Over 50 countries voted Netsafe's Chief Online Safety Officer, Sean Lyons, to become Vice President of the INHOPE global helplines network to combat child sexual explicit imagery distribution, a position he will hold for 2 years

MARCH

Launched Netsafe Lab working on research projects with international partners including the Alan Turing Institute

JUNE

Netsafe's Youth Action Squad launched their toolkit to schools, a youth-led resource to help young people lead online safety initiatives in their own school communities

NOVEMBER

Multi-award-winning **Porn Week campaign** in partnership with The Light Project and The Spinoff

APRIL

Released research into New Zealand's attitudes to mis/dis/Malinformation, a follow up to the 2020 "Your News Bulletin"

JANUARY

Launched our updated "kete" of materials for schools for Term 1

MAY

Launched the Xbox Gaming Toolkit for Families in partnership with Microsoft

FEBRUARY

Launched new online learning platform for schools including 6 micro learning modules co-designed with students and teachers

Our Impact

Netsafe is an independent non-profit organisation supporting people in Aotearoa to have safe and positive online experiences. We keep people of all ages safe online by providing free support, advice and education.

Over the past year, Netsafe received 23,213 reports of online harm, with April to June 2023 Netsafe's busiest ever quarter for complaints assessed as falling within the scope of the Harmful Digital Communications Act.



Reports of Online Harm

23,213

These reports spanned the full spectrum of online safety issues, including:



child sexual abuse



image-based abuse



scams



harmful hate speech



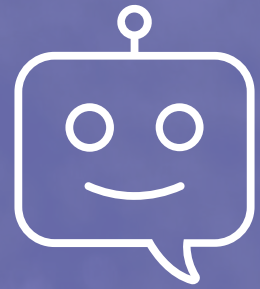
privacy breaches



digital parenting challenges



school incidents.



9,400

messages exchanged

between New Zealanders seeking
assistance with online harm incidents
and Kora, Netsafe's chatbot

Harmful Digital Communications

In 2016, Netsafe was appointed as the Approved Agency under the Harmful Digital Communications Act (HDCA). Our role and functions as the Approved Agency are to:

- to receive and assess complaints about harm caused to individuals by digital communications:
- to investigate complaints:
- to use advice, negotiation, mediation, and persuasion (as appropriate) to resolve complaints:
- to establish and maintain relationships with domestic and foreign service providers, online content hosts, and agencies (as appropriate) to achieve the purpose of this Act:
- to provide education and advice on policies for online safety and conduct on the Internet

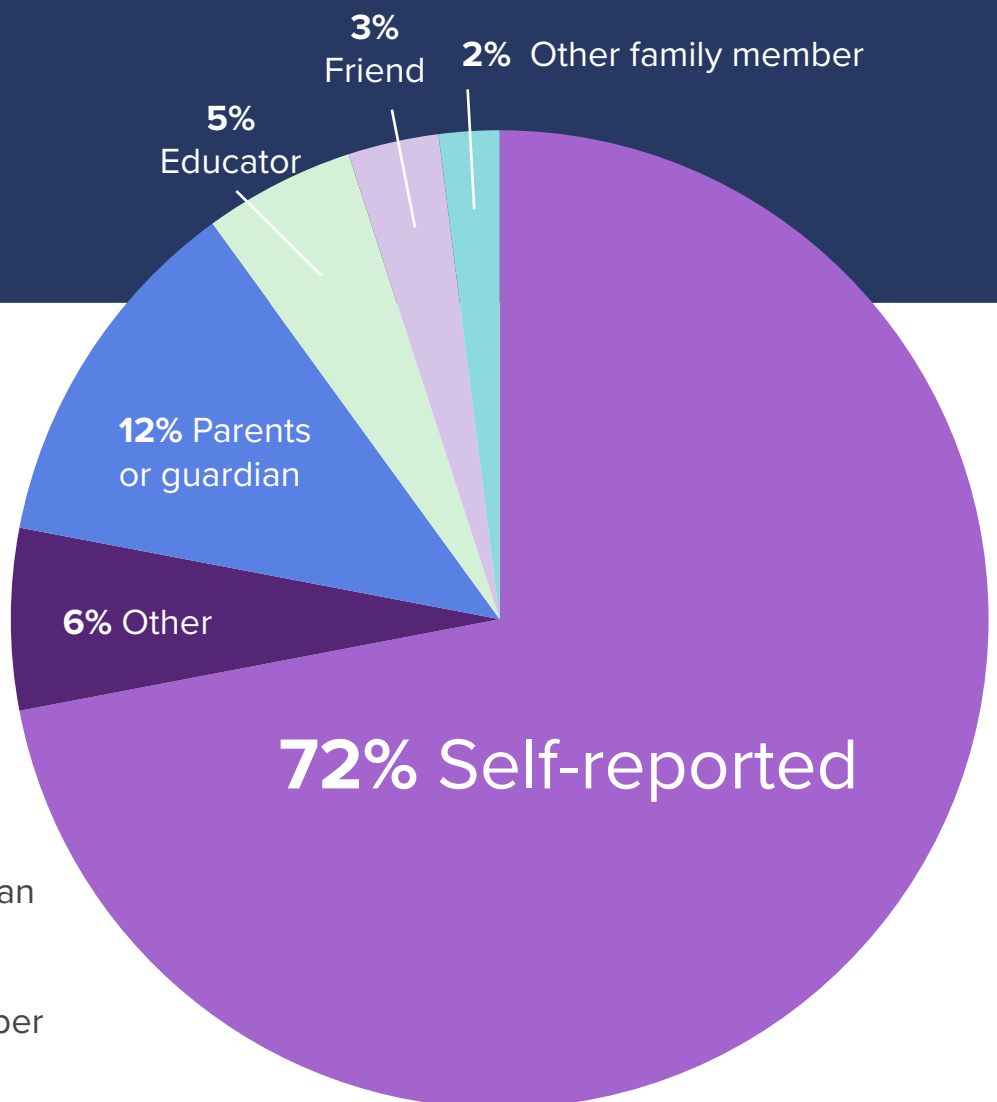
86.6%

Overall satisfaction rate

with Harmful Digital Communications service
from those surveyed over the year

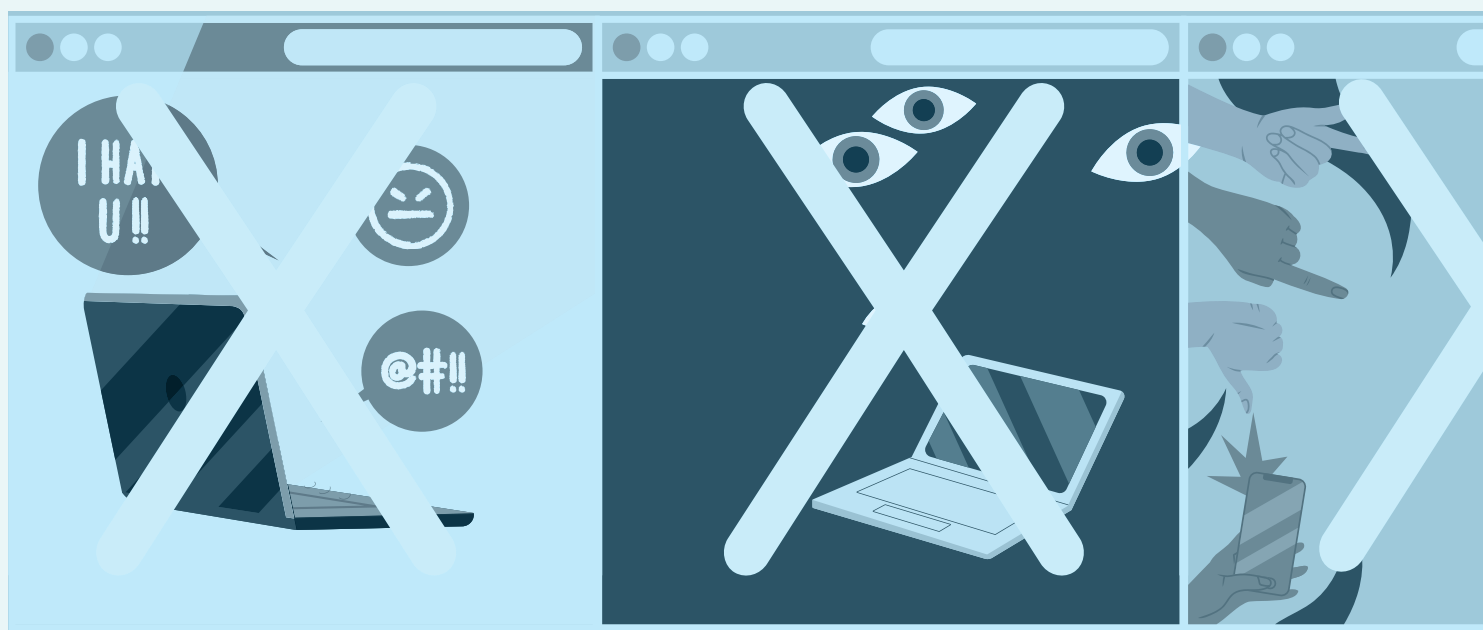
Total Harmful Digital Communications complaints received

5,023



Who is reporting?

72% Self-reported
12% Parents or guardian
6% Other
3% Friend
2% Other family member



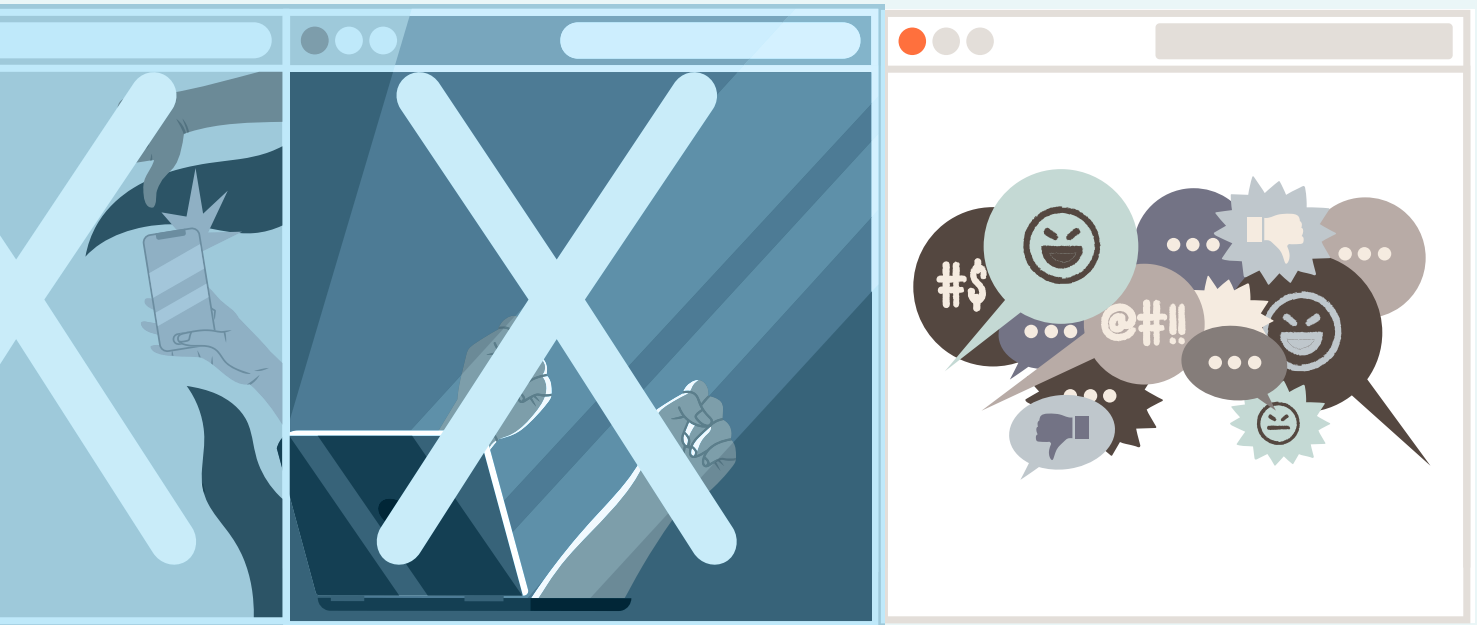
While we are able to assist the majority of people that come to Netsafe, not every report about online harm meets the criteria outlined in the Act.

We do our best to assist everyone who reports online harm, however, there are a number of circumstances where our ability to achieve a speedy resolution for the complainant is limited.

Some people are surprised to learn that we don't scour the internet for online harm or bad actors. A complaint must be brought to us before we can utilise the Approved Agency powers.

When the Act was written, phone calls were specifically excluded, on the basis that they were covered by the Telecommunications Act. Technological advances in messaging and communication apps such as Facebook Messenger, WhatsApp etc have blurred the lines between digital communications and telecommunications. For Netsafe to be able to apply its Approved Agency functions, a telephone call must be recorded digitally.

Hate speech targeting a group of people, mis and disinformation are examples of communications that are harmful, yet do not always identify an individual, and therefore, do not meet the current criteria defined in the Act. We continue to advocate for change in these areas to better protect vulnerable communities in New Zealand.



In simple terms, the communications principles, defined in the HDCA, state that a digital communication should not:

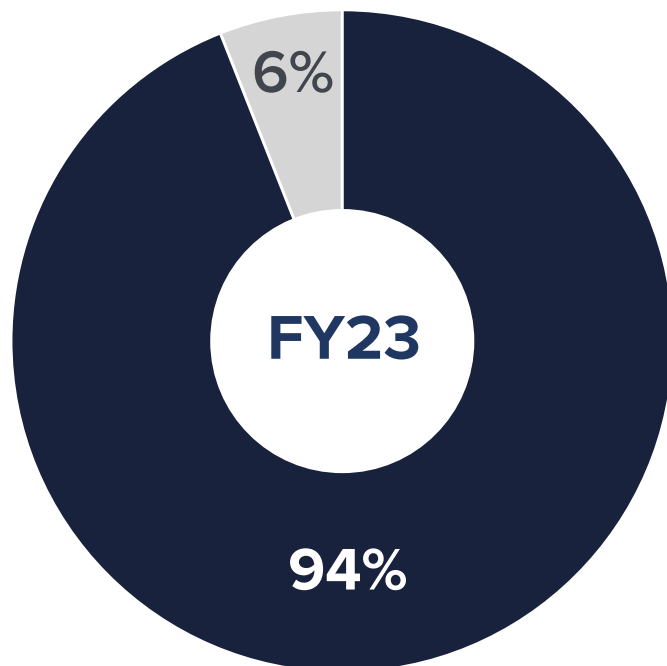
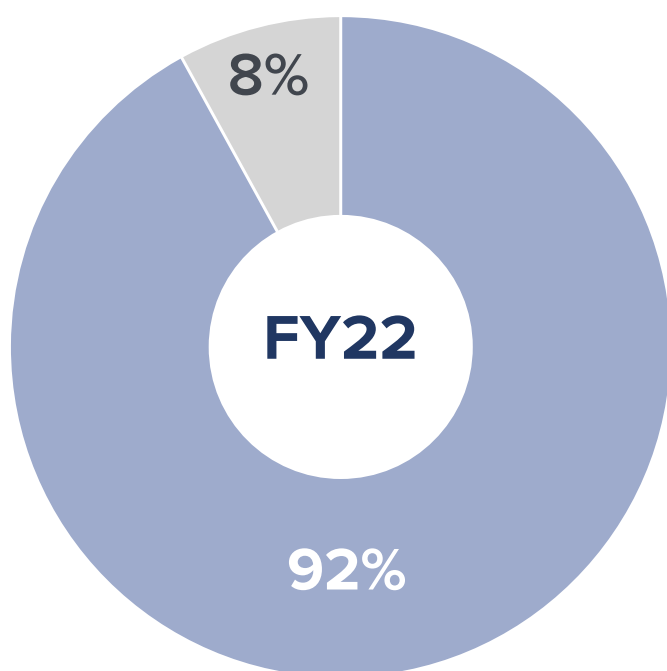
1. disclose sensitive personal facts about an individual
2. be threatening, intimidating, or menacing
3. be grossly offensive to a reasonable person in the position of the affected individual
4. be indecent or obscene
5. be used to harass an individual
6. make a false allegation
7. contain a matter that is published in breach of confidence
8. incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual
9. incite or encourage an individual to commit suicide
10. denigrate an individual by reason of colour, race, ethnic or national origins, religion, gender, sexual orientation or disability

HARMFUL DIGITAL COMMUNICATIONS

Resolutions and Timeliness

Harmful Digital Communications Act (HDCA) Resolution Rate

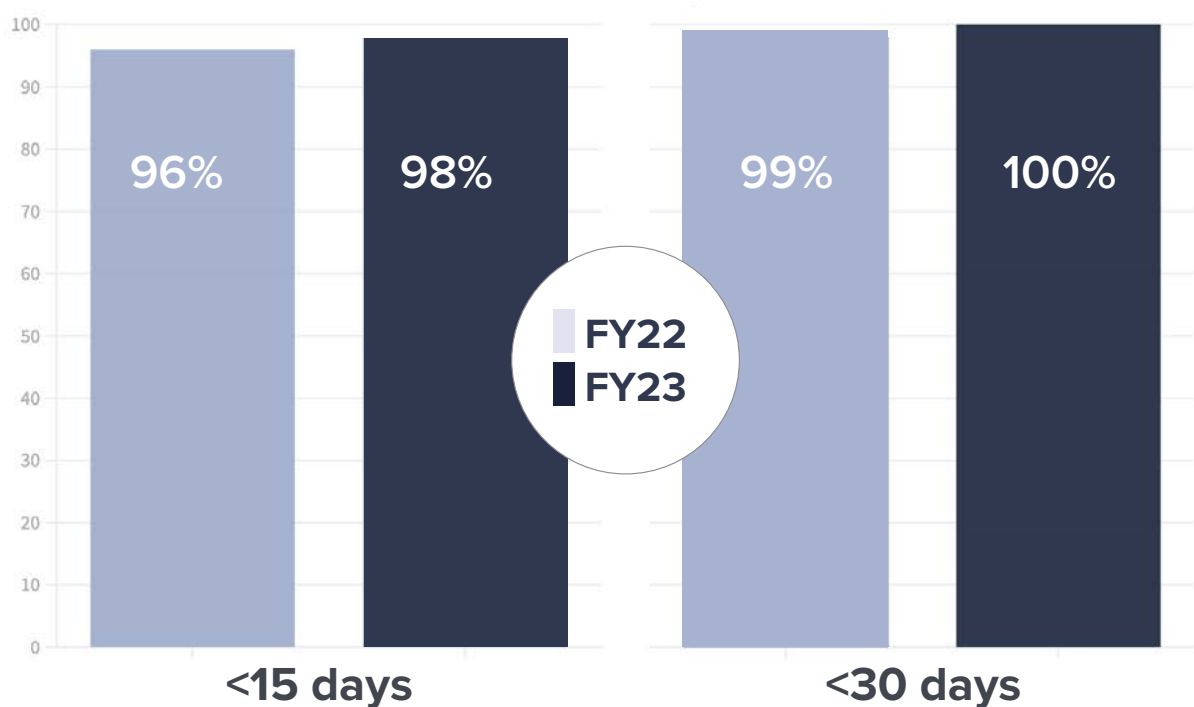
Netsafe's success rate at resolving HDC disputes improved in 2022/23 to 94% compared to the previous year.





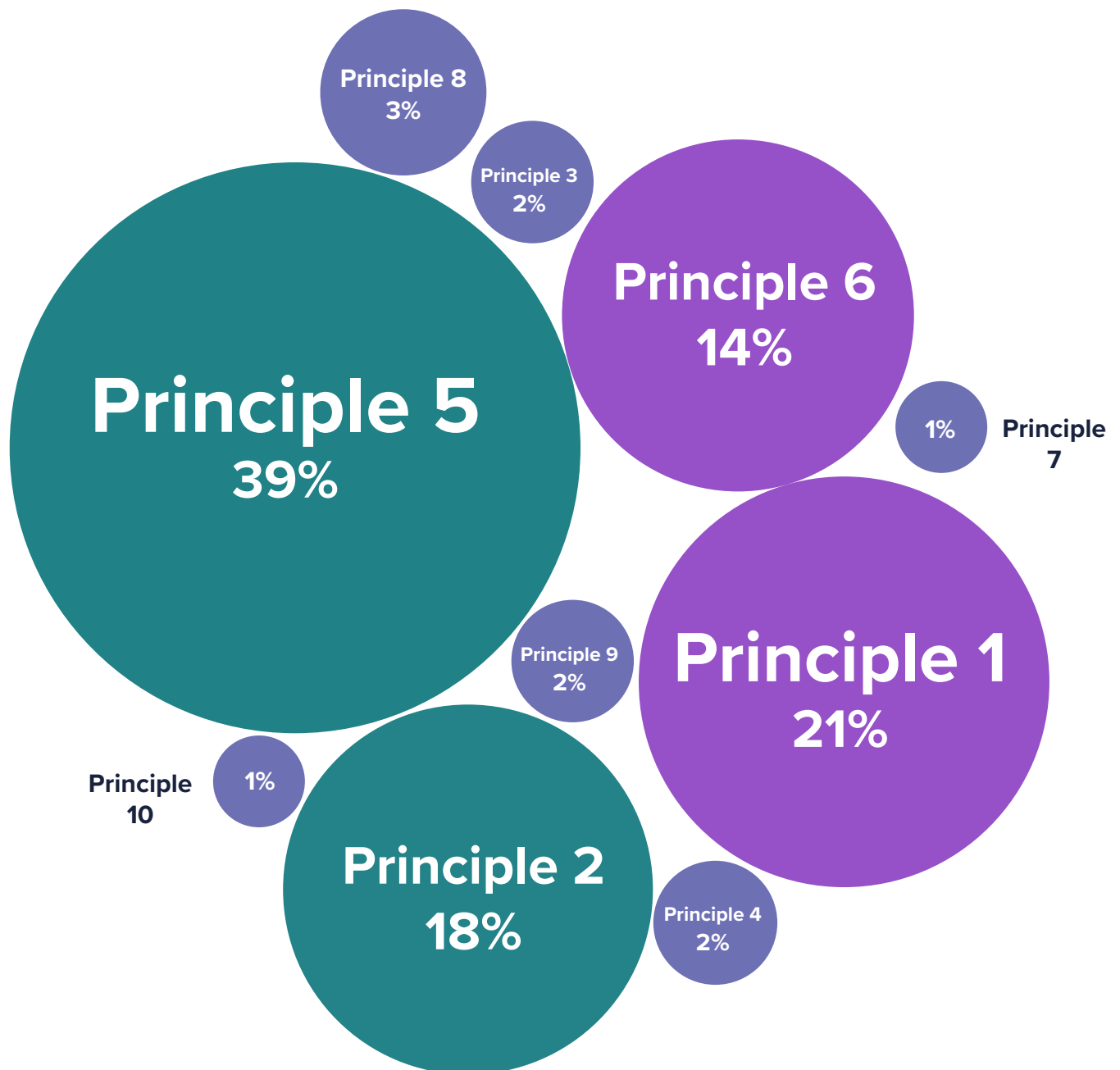
Timeliness of HDCA complaints completed

Timeliness of HDCA complaints completed. In 2022/23, 98% of all HDC complaints were resolved within 15 days, and 100% within 30 days



HARMFUL DIGITAL COMMUNICATIONS ACT

Reports by HDC Principle*



*For the purpose of this report percentages have been rounded up to the nearest whole number.

Complaints that breached one or more of the 10 communications principles:

3370

Principle	A digital communication should not	Reports	%*
1	Disclose sensitive personal facts about an individual.	694	21%
2	Be threatening, intimidating, or menacing.	534	16%
3	Be grossly offensive to a reasonable person in the position of the affected individual.	73	2%
4	Be indecent or obscene.	61	2%
5	Be used to harass an individual.	1309	39%
6	Make a false allegation.	472	14%
7	Contain a matter that is published in breach of confidence.	24	1%
8	Incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.	112	3%
9	Incite or encourage an individual to commit suicide.	59	2%
10	Denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.	32	1%

HARMFUL DIGITAL COMMUNICATIONS ACT

Case studies



1,707

REPORTS OF SEXTORTION

237%

Sextortion

In the year ended 30 June 2023, Netsafe received 1,707 reports of sextortion, a whopping 237% increase on the same period the previous year.

Sextortion is a form of blackmail where scammers threaten to share intimate images or videos unless their demands are met.

Usually, they demand money, but we have supported victims who have been extorted for more images or laundering money on behalf of the scammer. We know reports to Netsafe are just the tip of the iceberg as a significant number of cases go unreported due to victims' embarrassment, shame, fear of judgment, or fear of consequences.

Typically, scammers initiate a relationship with their victim via a mainstream platform such as Instagram, TikTok, Snapchat or Tinder. Often, they will request a switch to a secure messaging platform such as WhatsApp to protect the original account from being closed if the victim reports the online harm. This enables them to continue using accounts on mainstream platforms to target new victims.

Sextortion continued:

The scammer will share intimate images, supposedly of themselves, and encourage their target to share their own images. Once they receive intimate images from a victim, they threaten to share the images with the victim's friends, family or on public websites unless the victim pays them money. They often supply a screenshot of the victim's friends list from social media.

The amount of money requested varies between \$20 and \$2,000.

Our advice to victims is to stop all communication with the scammer. They are typically interacting with many victims concurrently, so they focus their attention on victims that have paid money or who continue to engage with them. In most cases, when communication stops the scammer moves on, without following through on their threat to share the images. However, there's no guarantee.

A large proportion of scammers are based overseas, and running this scam is how they earn a living.

Deep fakes

People creating deep fakes use real images, audio and video to digitally manipulate and generate artificial content that looks real. You can think of deep fakes as the 21st century's answer to photoshop. Most deep fakes are created using celebrities and other people in the public eye, where there is plenty of readily available content online.

However, Netsafe is receiving a rapidly increasing number of reports from everyday New Zealanders, including young people, impacted by deep fakes. The motivation for generating the deep fake is often bullying, revenge or humour, with the purpose of humiliating the victim. The content is often generated by someone known to the victim such as an ex-partner or former friend.

To the victim, it doesn't matter that the content isn't real. It looks real. And the impact is the same as though it were real.

Netsafe predicts that in the future, deep fakes will increasingly be used to blackmail victims, in the same vain as sextortion. In a recent experiment with a Netsafe employee, whose social media accounts were set to the highest privacy settings, it took just 3 minutes for a deep fake expert to locate an image of them on the internet and create a very realistic nude image. That expert predicts that within 3 years, 80% of people will be impacted by a deep fake of themselves.

Online Safety Operation Centre

Hardly a day goes by without a headline in the news about someone who has lost thousands of dollars in a scam. And for every story that makes it to the news, there are hundreds of others reported to Netsafe, and thousands more that go unreported.

Police data shows 93% of fraud and deception is not reported to the Police, and 97% of cybercrime is unreported.

Losses to scams over social media platforms amount to more than website, phone call, email, text or pop-up ad scams.

The most common social media scams are:

- fraudulent online shopping purchases
- fake investment opportunities
- romance scams.

Fraudulent online shopping purchases

The typical fraudulent online shopping scam involves high quality, branded products being offered at highly discounted prices. Clothing and electronic items such as phones are common items purchased but never arrive. To avoid getting caught up in this scam, Netsafe recommends you check feedback and reviews on the seller or search the seller's name plus "complaint" or "scam."

Fake investment opportunities

Whilst fewer people fall for fake investment scams, the amount of money lost is far greater. Scammers create a social media profile making them appear wealthy and credible. They may be offering courses or classes to help you get rich quickly.

Romance scams

Romance scams aren't new. The scammer initiates a friendship via a dating app or social media app and proceeds to "love bomb" the victim. This involves showering their victim with affection, flattery and attention. Some scammers are willing to play a long game, letting the charade continue for months. Once the victim becomes invested in the relationship, they request money, typically with high urgency.

Losses

Consumer investment fraud
\$9,294,229

Scam reports 604

Consumer products and services fraud
\$2,623,776

Scam reports 2789

Relationship and trust fraud
\$1,866,261

Scam reports 603

Scams
\$3,427,143

Scam reports 1749

Employment fraud
\$456,613

Scam reports 124

Prize and grant fraud
\$113,445

Scam reports 1640

Phantom debt collection fraud
\$59,077

Scam reports 314

Charity fraud
\$4,912

Scam reports 28

Sending spam
\$1,000

Scam reports 465

Total monetary loss from scams

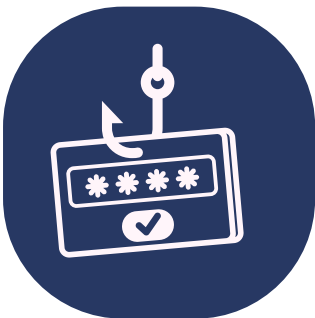
\$17,846,456

SCAM

Case studies



The most common scam types are:



Phishing



**Worthless or
non-existent
products or
services**



**Account
compromise**



Impersonation

These will capture approximately 90% of the scam incidents reported to Netsafe.



Phishing

Phishing is when someone tries to get personal information (like bank account numbers and passwords), from a large audience, so they can use it to impersonate or defraud people. These emails can look very real, and some scammers will even use the branding and logos of a legitimate organisation to make the email seem genuine.

Phishing scammers will contact many people in the hope that some of them will fall for the scam. These scam communications can seem like they are individually tailored, but in reality, the same scam is being sent to hundreds, if not thousands of people at the same time.

Phishing scammers will often claim to be from a legitimate organisation, or to

have some kind of 'deal' to be claimed. For example, a scammer may send out an email telling people they have won a lottery, and to claim the winnings they need to provide some details. Other phishing scams use scare tactics, where the scammers pretend to be lawyers or employees of the government and threaten legal action if you don't give them information or money. We've also received reports regarding scam emails claiming that online accounts or memberships have been cancelled, have expired or have details that need updating.

In the year ended 30 June 2023, we received nearly twice as many scams involving worthless or non-existent products and services than any other scam. Unfortunately, it can be difficult to get money back that has been lost in one of these scams.

Engagement

(events, partnerships, marketing)

Events

Netsafety Week

Netsafety Week 2022 created space for diverse conversations about culture and online safety, including with Māori communities (x3 networking breakfasts and x10 webinars).

Webinar and community events

We delivered a webinar on young people and privacy online, as part of the Privacy Commissioner's Privacy Week.

Six Netsafe LIVE community events were hosted in Gisborne, New Plymouth, Pakuranga, Rotorua, Rolleston and Northland.

Research and Media

In December 2022 and January 2023 Netsafe commissioned first of its kind research into mis and disinformation in New Zealand. We released our research into New Zealand's attitudes to mis/dis/Malinformation as a follow up to the 2020 "Your News Bulletin" campaign.

This year Netsafe achieved 526 pieces of media coverage, an average of 43 stories per month, including 35 on broadcast TV. Top media channels included some of the widest-reaching platforms in New Zealand from 1 News through to the Herald, Stuff, RNZ National and The Spinoff.

91%

of New Zealanders
are experiencing
misinformation at
least MONTHLY

79%

of New Zealanders
are experiencing
misinformation at
least WEEKLY

47%

of New Zealanders
are experiencing
misinformation at
least DAILY

New Zealand's attitudes to mis/dis/Malinformation, 2023



Presentations

Netsafe presented globally at the following international events in person and online including:

- Panel on the regulation of social media in Sri Lanka highlighting the New Zealand Code of Practice for Online Safety Harms – support request from the High Commission in Colombo
- Virtual dialogues on the Frontiers of Digital Economy, organised by LIRNEasia: How the Aotearoa New Zealand Code of Practice for Online Safety and Harms works
- Meta's first Asia Pacific Mixed Realities Summit in Singapore
- Asia Internet Coalition Online Safety Forum at Lee Kuan Yew School of Public Policy Singapore. Panel discussion on self-regulation and The New Zealand experience. An overview of the drafting and adoption of the self-regulatory model in New Zealand.
- GIFCT and Meta countering violent extremism presentation, Singapore
- ICANN, Washington workshop on countering child sexual exploitation materials
- Facebook Oversight
- Internet Corporation of Assigned Names and Numbers meeting, the Internet Governance Forum of Taiwan
- International Symposium on Cyberbullying



Partnerships

Bodyright.co

Award-winning Bodyright.co partnership campaign for Mental Health Awareness Week #BeYourSelfie encouraging young New Zealanders to think about the impact of their use of filters on their images.

Domain Name Commission

Partnered with Domain Name Commission to launch a safer online shopping factsheet for Fraud Awareness Week.

Protect Children Europe

To mark Best Friends Day, we partnered with Protect Children Europe launching the #MyFriendToo campaign, encouraging young people to tell an adult if their friend is experiencing image-based abuse.



PORN WEEK



Campaigns

Porn Week

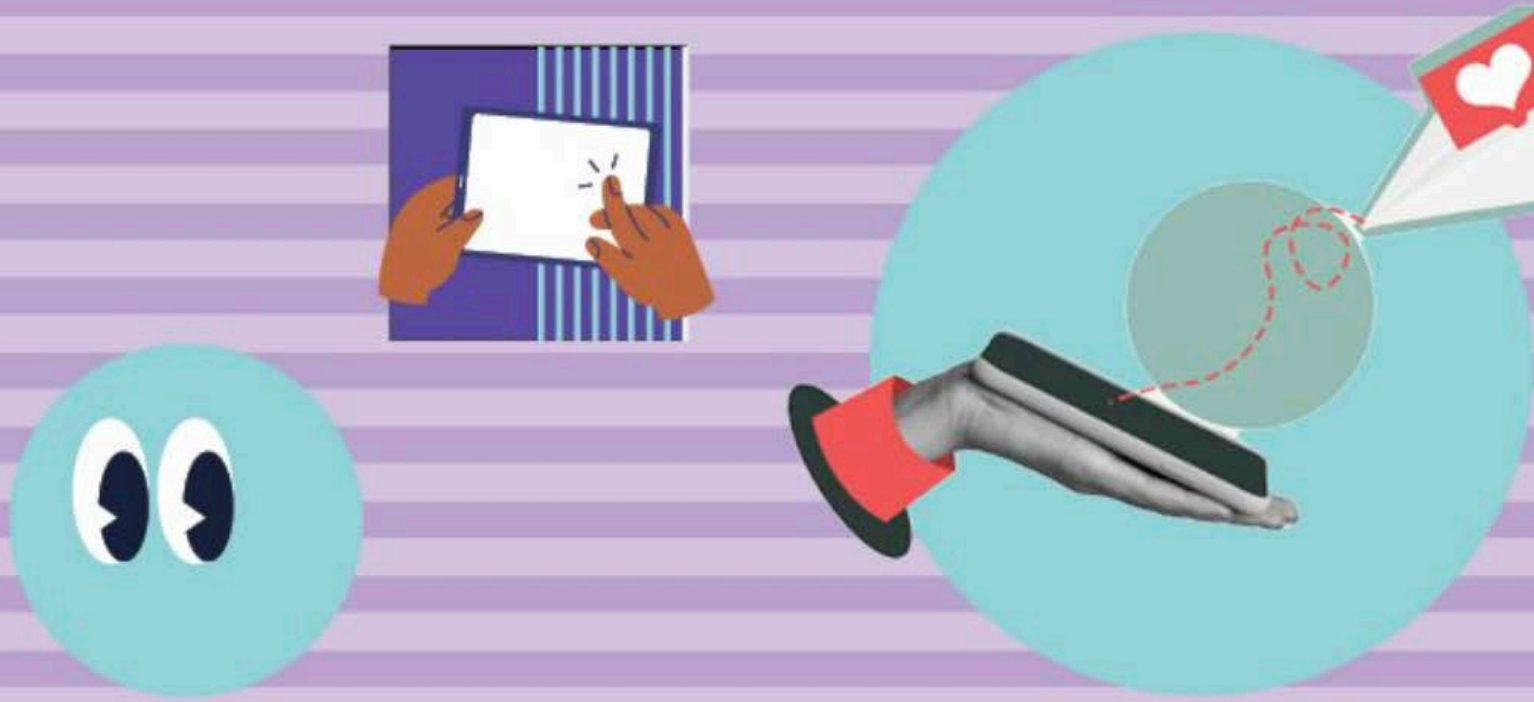
Multi-award-winning Porn Week campaign in partnership with The Light Project and The Spinoff, to create a nationwide conversation about online pornography and its impact in the non-consensual image-sharing space. The Spinoff articles sent 1,200 visitors to our dedicated education microsite, which itself saw another 4,000 visits during launch week, collecting 75 personal submissions from young New Zealanders.

Safer Internet Day

We hosted Safer Internet Day 2023 in New Zealand with the website seeing 111 organisations sign up to support and the campaign receiving 14 pieces of media coverage. Netsafe ads ran on Spotify reaching 98,000 teenagers in New Zealand.

“Freshers”

Netsafe ran a “freshers” campaign to new university students in Semester 1, with sextortion, harassment and phishing messages running in all 6 university student magazines, resulting in 44 harm reports from the 18-29 age group.



Education

GovTech accelerator:

We joined the GovTech accelerator programme to learn co-design best practice in the creation of our first suite of online learning modules in schools.

Alannah & Madeleine Foundations' Digital Licence:

We launched the Alannah & Madeleine Foundations' Digital Licence product into New Zealand schools, with 72 schools registering for 13,580 free student licences.

Updated Kete:

In preparation for Term 1, we launched our updated "kete" of materials for schools which included student user agreement templates, staff guidelines, digital safety management plans and a guide to responding to digital safety incidents.

New Youth Action Squad cohorts:

We welcomed a new cohort of our Youth Action Squad, including young people from the regions outside of Auckland for the first time.

New online learning platform:

Netsafe launched a new online learning platform for schools that has welcomed 2,000 learners who have completed 3,525 assignments across the pilot range of six micro learning modules aimed at Years 9-11.

Youth Action Squad Toolkit

Our Youth Action Squad launched their toolkit to schools, a youth-led resource to help young people lead online safety initiatives in their own school communities.

Kia ora and welcome to the squad!

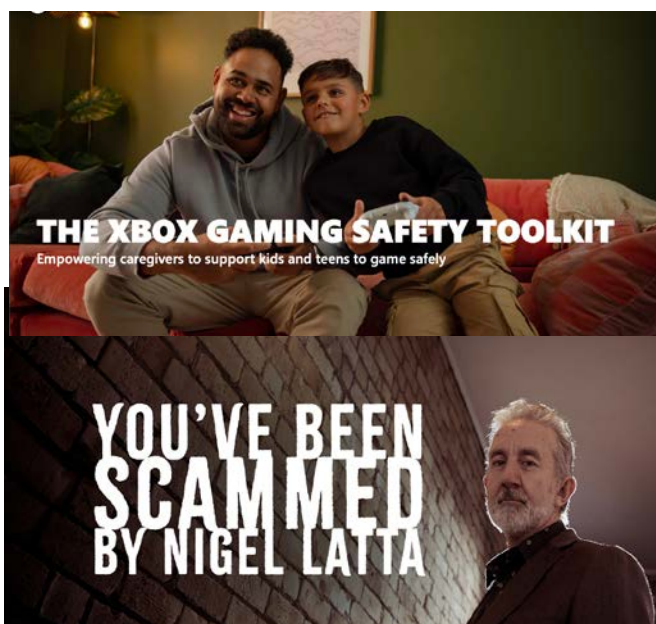
Spending time online should be a safe and positive experience for young people. That's where Netsafe's Youth Action Squad (YAS) comes in.

[LEARN MORE](#)



Xbox Gaming Toolkit

We also launched the Xbox Gaming Toolkit for Families in partnership with Microsoft and other Australian and New Zealand organisations. The Toolkit builds on Netsafe's original Gaming Toolkit for Whanau, with bespoke advice for parents with Xbox platforms in the home.



Documentary series

We also participated in the "You've Been Scammed" documentary series with Nigel Latta on TVNZ to expose scammer techniques to the public and help prevent harm.

School and Community Workshops

Our education team travelled the length and breadth of New Zealand to deliver 165 school sessions this year, in 101 locations nationwide, reaching 4,037 teachers and parents. We exhibited at 6 industry conferences to educate school leaders and we partnered on community education events with various organisations both inside the education system (e.g. N4L, New Era, Life Education Trust) and in the community (e.g. Police Youth Aid, Whanau Ora, Deaf Aotearoa, Shakti).

Our Priorities

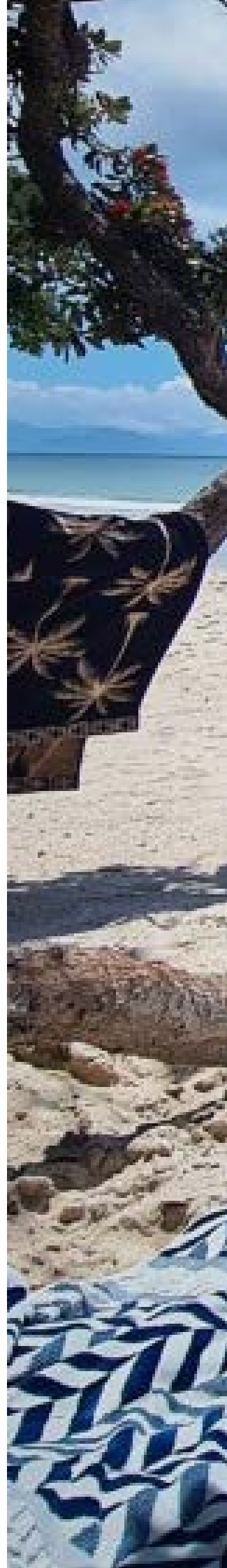
(2024 Outlook)

Netsafe must adapt to the rapid transformation of New Zealand's online environment, facing significant opportunities and immediate challenges. The HDCA requires modernisation to align with the current online landscape, distinct from its state in 2015 when the Act was enacted.

In the upcoming year, key focus areas include understanding the evolving operating environment with a new government, prioritising anti-scam efforts with a consumer focus, adjusting education initiatives to a new curriculum, and balancing innovation and automation while ensuring efficient dispute resolution within 10 working days and high user satisfaction.

Netsafe's agenda involves enhancing regulatory settings for online safety, advancing Te ao Māori approaches, and establishing new partnerships through Netsafe Lab. There's a commitment to delve deeper into the education sector by introducing online safety products for a younger audience and conducting various awareness campaigns throughout the year, such as Safer Internet Day and Netsafety Week.

Crucially, Netsafe aims to anticipate future technological developments, ensuring support for all individuals in New Zealand to have safe and positive online experiences. This vision involves reconnecting globally with the online safety community, with a particular emphasis on the Pacific as a key geography for the next 18 months and an integral part of our outreach agenda.







Legislation and Compliance

We are committed to protecting the confidentiality and integrity of our service.

To help people successfully, Netsafe needs them to openly disclose sensitive information and trust that we will protect the information they share with us.

We endeavour to comply with the Ombudsmen Act 1975, Official Information Act 1982, Public Records Act 2005, and Privacy Act 2020.

The table below outlines the requests for information (RFI) under the Official Information and Privacy Acts. Netsafe will refuse requests where we believe we are justified in doing so. For example, where we believe the disclosure would involve the unwarranted exposure of another person's information. This can be the case where an author of alleged harm requests information provided to Netsafe by the person who has been the target. When we do refuse, requesters can exercise their right to complain to the Privacy Commissioner or the Ombudsman about the decision.

	FY22	FY23
Requested for Information (RFI) requests received.	33	27
Withdrawn requests.	4	2
Requested for Information (RFI) timeframe met.	27/29	25/25
Complaints to Office of Privacy Commissioner or Ombudsman.	2*	0*

*A complaint to the Ombudsman previously indicated in FY22 was formally received by Netsafe in FY23. This complaint is now counted in FY23 as opposed to FY22.



Financial Highlights

Netsafe's financial statements were audited by Grant Thornton New Zealand Ltd. Outlined below is a summary of Netsafe's financial highlights. All figures provided are excluding GST.

Revenue

For the 12 months from 1 July 2022 to 30 June 2023, Netsafe's total revenue was **\$5,667,668**.

Expenditure

The total expenditure for the 2022/2023 financial year was **\$4,851,169**.

Surplus/Deficit

In line with expectations, Netsafe achieved a Net Profit of **\$846,688**. This surplus has been held in cash reserves to provide for future investment to grow the business.

Funding

Netsafe has a meaningful level of autonomy and independence from its funding partners.

Statement Of Consolidated Revenue And Expenditure

	FY23	FY22
Revenue		
Revenue from exchange transactions	5,640,668	4,418,646
Revenue from non-exchange transactions	27,000	400
Total revenue	5,667,668	4,419,046
Expenses		
Administration expenses	235,069	255,568
Audit fees and consulting fees	497,771	588,723
Other operating expenses	1,104,423	682,774
Staff expenses	191,602	268,488
Wages and salaries	2,822,304	2,891,422
Total expenses	4,851,169	4,686,974
Finance income		
Interest, dividends and other investment revenue	30,189	2,758
Total finance income	30,189	2,758
Net surplus/(deficit) for the year	846,688	265,170
Total comprehensive revenue and expenses for the year	846,688	265,170

Statement Of Consolidated Financial Position

	FY23	FY22
Current Assets		
Cash and cash equivalents	1,822,856	1,165,866
Receivables from exchange transactions	1,125,193	697,581
Goods and services tax	-	-
Total current assets	2,948,049	1,863,448
Non-Current Assets		
Property, plant and equipment	119,694	76,781
Total non-current assets	119,694	76,781
Total Assets	3,067,743	1,940,228
Current Liabilities		
Payables from exchange transactions	224,539	100,159
Employee benefits	336,331	227,974
Goods and services tax	673	25,817
Income in advance	184,783	111,549
Total current liabilities	746,325	465,498
Total liabilities	746,325	465,498
Total net assets	2,321,418	1,474,730
Equity		
Accumulated surpluses	2,321,418	1,474,730
Total equity	2,321,418	1,474,730

Connect to Netsafe

Stay Informed

- Follow Netsafe NZ on Twitter, Facebook, LinkedIn, Instagram and TikTok
- Subscribe to Netsafe updates at netsafe.org.nz/newsletter
- Use **netsafe.org.nz** as a one-stop online safety resource

Become a Member

- Help advance online safety in NZ
- Membership is free. Apply at netsafe.org.nz/member
- Email **membership@netsafe.org.nz** with any queries

Support Netsafe

- You can contribute financially or in kind to Netsafe
- givealittle.co.nz/org/netsafe
- Email **outreach@netsafe.org.nz** to learn more

Share Knowledge

- Netsafe's team are available to share their expertise and our data insights with the media
- Email **outreach@netsafe.org.nz** with queries

Annual Report Queries

- Enquiries about Netsafe's 2023 Annual Report can be emailed to **outreach@netsafe.org.nz**