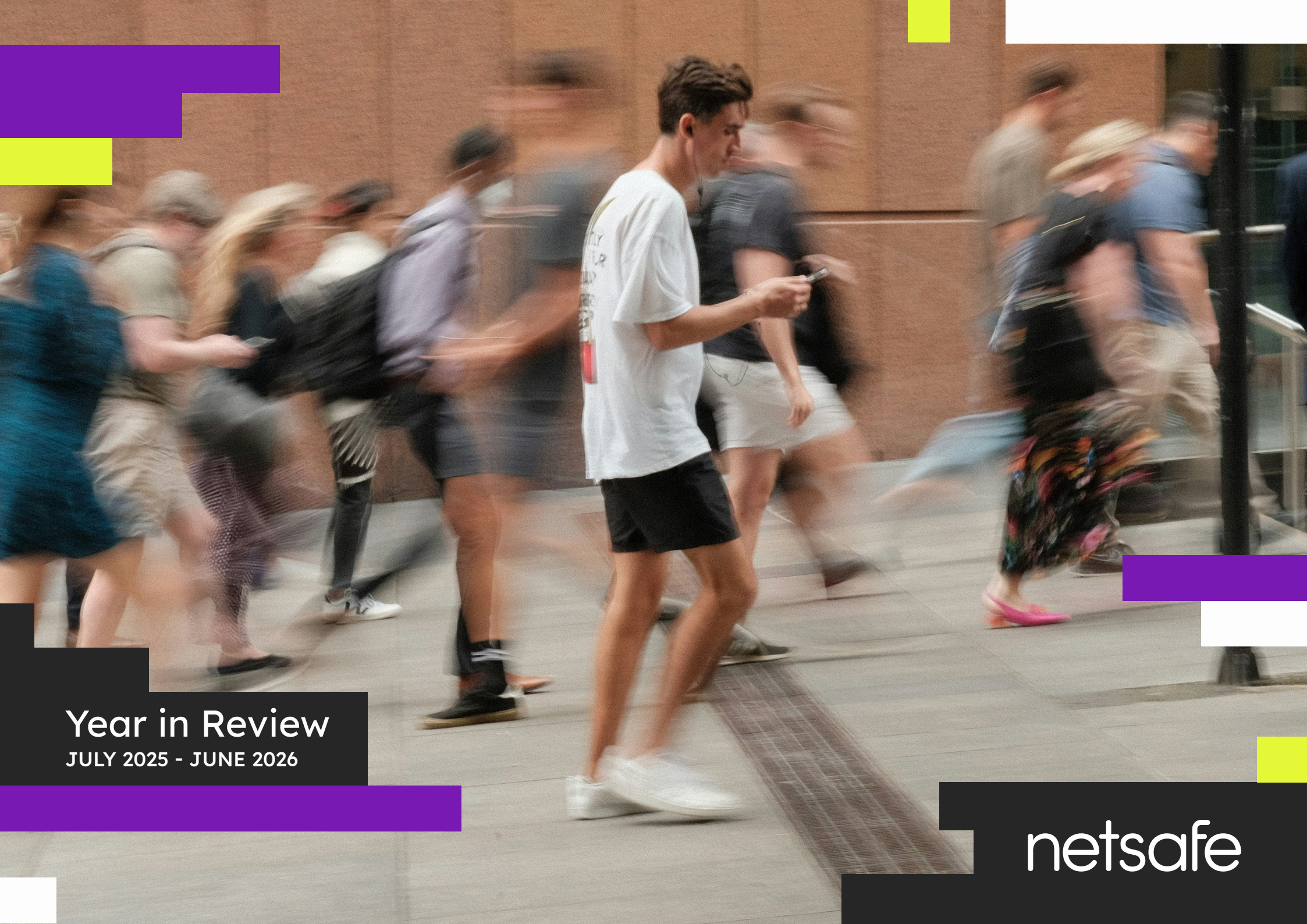


Year in Review

JULY 2025 - JUNE 2026

netsafe

Contents

Chair's Foreword 3
Chief Executive Officer's Report 4
How Netsafe Makes a Difference 6
FY26: Year at a Glance 7
Our Helpline Service 9
Our Harmful Digital Communications Service 10
Reporting Overview 11
Scams Helpline: Responding to Scams and Fraud 15
Netsafe Lab: Building Technology for Public Good 16
Protecting Children against Child Sexual Abuse Material 18
Recognised for Service Excellence 19
Education: Supporting Safer Schools & Kura 20
Public Education: Harm Prevention in Partnership 23
Turning Research Evidence into Actions 28
Reaching Communities Where They Are 31
Global Ideas, Engagement and Impact 33
Influence, Advocacy and Systems Change 37
Our Priorities for the Year Ahead 39
Legislation and Compliance 40
Financial Performance 41
Appendices 45

Chair's Foreword

Netsafe's governance must keep pace with the scale and complexity of the harm it is asked to respond to. My focus as Chair this year has been the three things the Board exists to protect — Netsafe's independence, its financial sustainability, and its ability to serve New Zealanders for the long term. This year tested all three.

Demand for Netsafe's services continues to outpace secure, ongoing funding. This is a governance risk as much as an operational one. The Board has worked closely with the executive to ensure Netsafe's sustainability does not rest on goodwill, short-term contracts or one-off contributions.

The Board's attention has also been on the operating model itself: strengthening Netsafe's ability to adapt to changes in funding or operating conditions without compromising the services New Zealanders depend on most. The work is underway and will continue into the coming year.

Sustainability cannot come from any single source. Government, industry, iwi, philanthropy and civil society each hold part of the responsibility — and part of the opportunity — for ensuring New Zealanders have somewhere to turn when online harm occurs.

In December we farewelled Claire Amos and Colin James. Both gave significant service to Netsafe over many years and their contribution to the organisation has been substantial. On behalf of the Board, I thank them. We welcomed Alicia Lemmer and Ian Olan, who bring a broad range of skills and experience to the Board table.

My thanks to my fellow directors for their stewardship, and to our Chief Executive, Brent Carey, and the Netsafe team for their professionalism, care and dedication. Their work is challenging, often complex, and deeply human. The Board is proud to support an organisation that continues to earn the trust of New Zealanders.



Dr Warren Williams
Netsafe Chairperson

Chief Executive Officer's Report

Online safety is changing quickly, and Netsafe's role has never been more important.

We received 27,482 online harm reports, including a record 7,792 under the Harmful Digital Communications Act, during the year in review. This reflects rising demand and increasingly complex, interconnected harms.

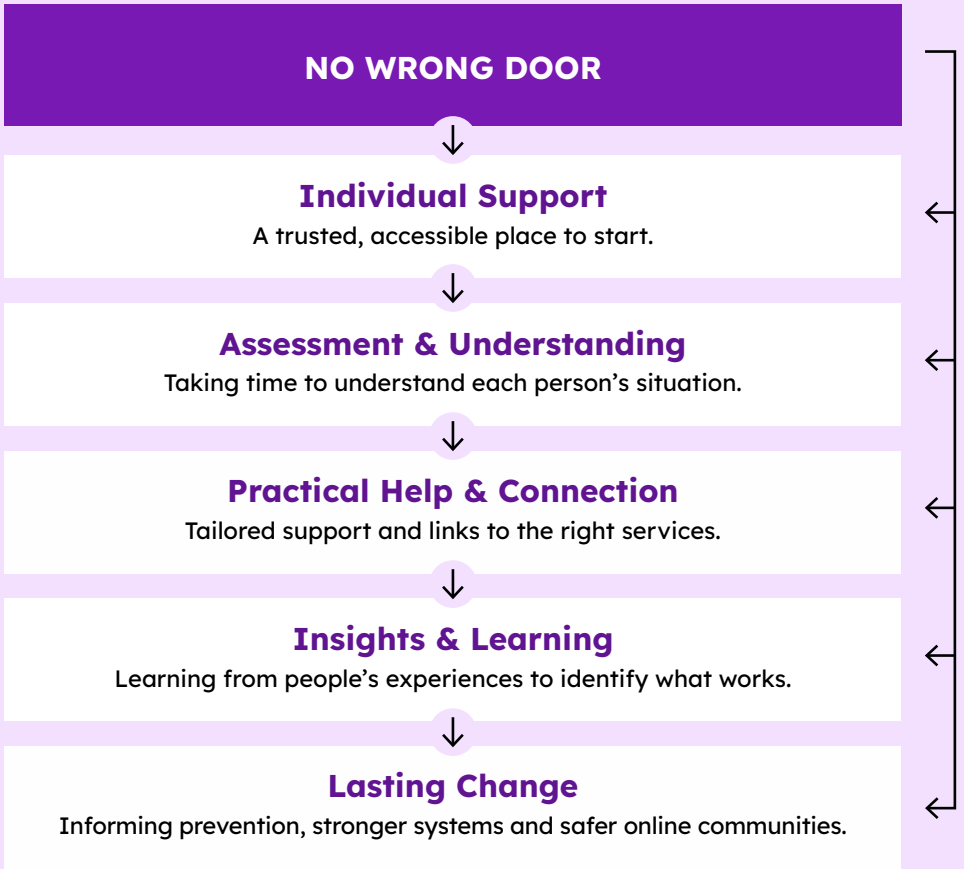
Despite this growth in demand, more than nine in ten HDCA complaints were resolved without District Court involvement and most matters were completed within 15 business days, indicating timely human support can make a difference.

Artificial intelligence, synthetic media, scams, sextortion, online abuse and harmful content are reshaping the online safety landscape. Scams are becoming more convincing, abuse more scalable, deception more personal, and deepfakes are moving rapidly from emerging risks to everyday realities.

Legislative responses, such as the Deepfake Digital Harm and Exploitation Bill and new stalking laws, are encouraging, but New Zealand's ten-year-old Harmful Digital Communications Act needs modernising, so protections keep pace with the harms people now face.

This year, Netsafe continued to adapt. We combined technology with human judgement and made deliberate choices about where to focus for the greatest impact. With finite resources, rising demand and essential services like scams lacking secure funding, we reshaped services and focused on where our helpline, education and digital safety tools made the greatest difference.

A central part of Netsafe's future is becoming New Zealand's trusted "No Wrong Door" for reporting online harms. People do not experience online harm in neat categories: a scam can become a mental health crisis, online abuse a wellbeing issue, and a deepfake image-based abuse. People should know there is one trusted place to turn, regardless of how digital harm presents itself.



Our reappointment as the Approved Agency under the Harmful Digital Communications Act for a third term reflected confidence in Netsafe's services and direction.

Our work also continued beyond New Zealand through international policy, Pacific capability-building and relationships with regulators and civil society organisations from around the world. These connections matter because digital harm crosses borders, and safer online environments depend on shared learning and coordinated responses.

Looking ahead, online safety is becoming less about technology alone and more about trust. As artificial intelligence reshapes how we live, work and connect, people will increasingly need non-governmental organisations they can rely on when something goes wrong.

Trust cannot be downloaded or automated; it must be built, protected and earned over time.

To our Board, staff, government partners, funders, donors, corporate supporters and the many organisations working alongside us: thank you. Your expertise, generosity and commitment make this work possible.



Brent Carey
Chief Executive Officer

How Netsafe Makes a Difference

Netsafe is New Zealand's independent frontline online-safety organisation. We provide practical support when harm occurs, help people and communities prevent harm earlier, and use evidence from our services to help improve the systems shaping digital life. Our ambition is to become New Zealand's recognised No Wrong Door for reporting online harm—one trusted place where people can begin, regardless of how that harm presents itself.

27,482

ONLINE HARM REPORTS RECEIVED

Trusted support when people needed somewhere to turn.

14,744

SCAM AND FRAUD REPORTS

Helping people take practical steps to reduce further harm.

1,503

SCHOOLS REACHED

Extending trusted online-safety support across Aotearoa.

31,717

KETE RESOURCES DOWNLOADED

Equipping educators with practical online-safety learning.

22

PACIFIC FACILITATORS TRAINED

Building locally led online-safety capability across the Pacific.

34,039

DIGITAL GUARDIAN GUIDE USERS

Helping parents and whānau navigate children's online lives.

FY26: Year at a Glance

Our impact extends beyond individual cases. Frontline experience informs Netsafe's education, research, policy advice, platform engagement and prevention work, turning what people tell us into improvements across the wider online-safety system.

28 JULY–
1 AUGUST
2025

JULY

Netsafety Week: Power in Partnerships

65+ library resource packs shared nationwide extending practical online-safety information to older people, teenagers and te reo Māori audiences across the motu.



AUGUST

Headspace Invaders launches

Headspace Invaders digital campaign reaches 330,000 young people. Raising awareness of critical thinking when encountering misinformation and radicalisation content online.



SEPTEMBER

Kete's educator community grew

Learning extended to 1,503 schools and more than 17,000 student sessions.

Q1

OCTOBER

Netsafe's frontline quality was nationally recognised

Five NZ Contact Centre Awards recognised service quality and innovation.



NOVEMBER

State of Scams revealed the scale of harm

$3b lost nationally to scams, up 30% from 2024, used in media commentary and outreach for scale of the problem.

82%

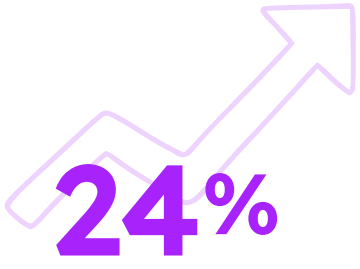
of New Zealand adults have encountered a scam

DECEMBER

Netsafe kept support timely through the end of the year

Between October and December the helpline handled 6,410 reports, including 3,390 scam and fraud reports, and 97.01% of HDCA matters were completed within 15 business days, our best result of any quarter in FY26.

Q2



JANUARY

Netsafe responded to a summer sextortion rise

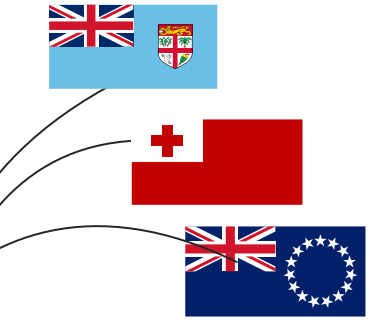
We used our report intelligence to identify a 24% rise in reports to update online guidance and deliver a summer awareness campaign, helping people recognise coercion, preserve evidence and seek support earlier.



FEBRUARY

Cyberbullying prevention support launched for schools

Toolkit supports Years 1–13; almost 4,000 users since launch.



MARCH

Confident & Connected digital safety train the trainer programme

Delivered across Cook Islands, Tonga and Fiji and gifted to Pacific Island partners to run themselves.



APRIL

Reports highlighted the cost of investment scams

Investment scams reported to Netsafe cost people $1.23 million in the 12 months to April, an average of $14,800 per report, giving Netsafe timely intelligence to strengthen public warnings and inform our scam-prevention advice.



MAY

Digital Guardian Guide strengthened whānau support

34,039 unique users; 54,691 sessions; earned a 4.4/5 rating for free practical support to parents and whānau.



JUNE

Netsafe informed deepfake law reform

Netsafe evidence cited by Parliament and reflected in proposed next steps on HDCA reform, platform accountability and New Zealand based research.

Q3

Q4

Our Helpline Service

Netsafe's helpline team provides free advice and support to people experiencing a wide range of online safety issues.

For people experiencing online harm, practical clarity can be an important outcome: understanding what happened, what can be done next and where further protection or redress may be available.

In FY26 we received 27,482 online harm reports, showing both the scale of need across Aotearoa New Zealand and the continued importance of having an independent, trusted place for people to turn when online harm occurs.

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

- child sexual abuse material
- image-based sexual abuse
- scams
- hate speech
- online harassment
- AI-generated abuse
- privacy breaches
- digital parenting challenges
- school incidents

This breadth of harms is why New Zealand has a No Wrong Door service in Netsafe as people should not have to consider the category of harm before they can report and find the right help.

Netsafe helped thousands of New Zealanders regain control of their online lives. Demand reached a record level, including 7,792 complaints under the Harmful Digital Communications Act and 14,744 related to fraud or other scams.



Our Harmful Digital Communications Service

In 2016, Netsafe was first appointed as the Approved Agency under the Harmful Digital Communications Act (HDCA).* Netsafe takes and assesses complaints about harm caused to individuals by digital communications.

In FY26, Netsafe assessed 7,792 complaints as engaging the thresholds of the HDCA, compared with 6,404 HDCA complaints in FY25. This was Netsafe's busiest year to date, representing a 22% year-on-year increase.

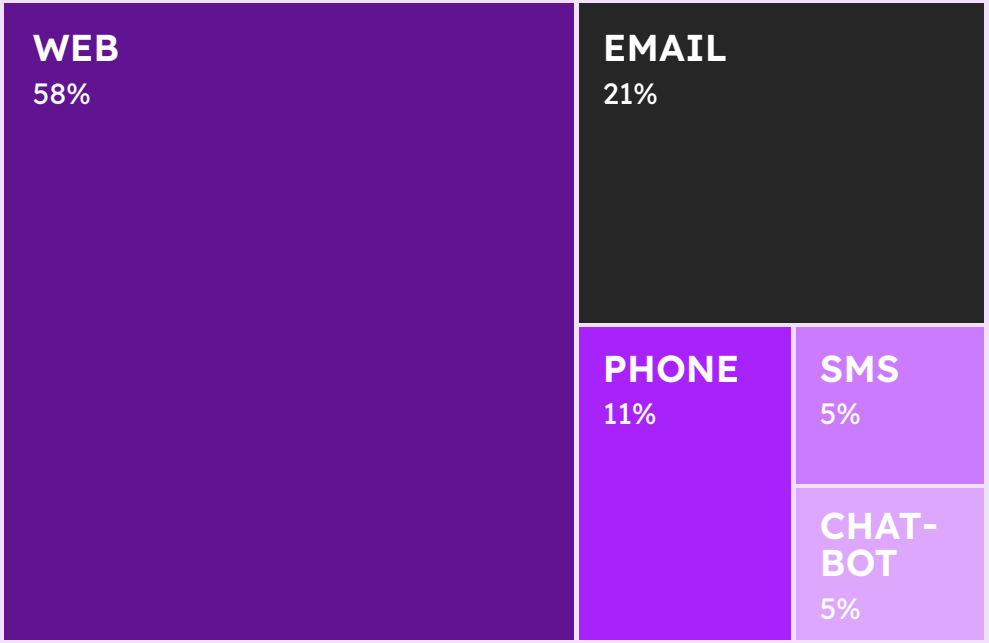
The April to June 2026 quarter was our busiest ever quarter for complaints assessed as falling within the scope of the HDCA.**



22% increase

of HDCA complaints from FY25 to FY26

REPORTS RECEIVED BY CHANNEL



*The functions of the Approved Agency are:

(a) to receive and assess complaints about harm caused to individuals by digital communications:

(b) to investigate complaints:

(c) to use advice, negotiation, mediation, and persuasion (as appropriate) to resolve complaints:

(d) 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:

(e) to provide education and advice on policies for online safety and conduct on the Internet:

**We assist everyone who reports online harm to Netsafe, irrespective of whether these thresholds are met.

Reporting Overview

Who is reporting and from where?

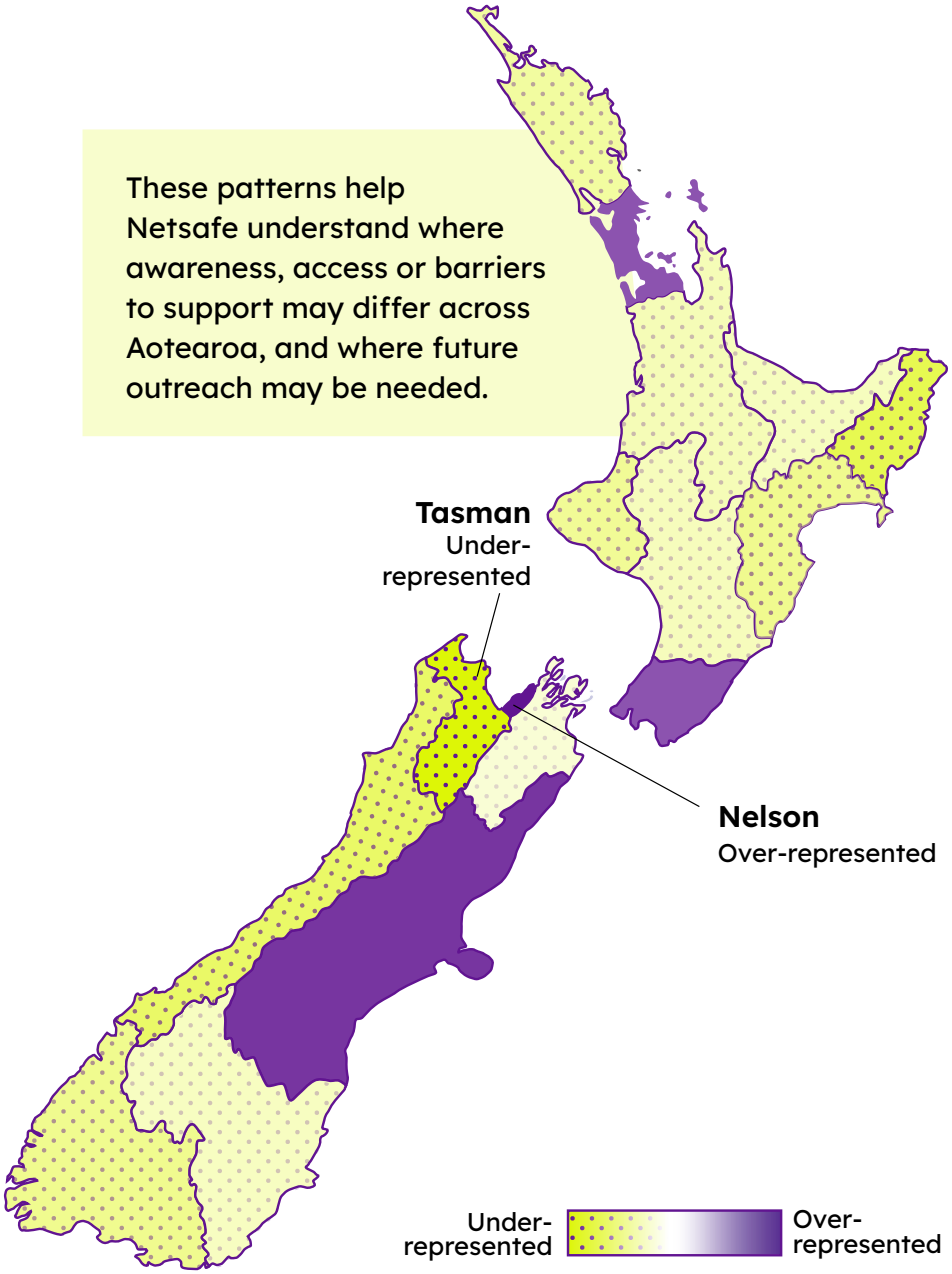
SELF REPORTED	86.75%

REPORTING ON BEHALF OF SOMEONE ELSE

PARENT/GUARDIAN	6.13%
OTHER	2.16%
OTHER FAMILY	1.72%
EDUCATOR	1.59%
FRIEND	1.57%
NZ POLICE	0.08%

Regional reporting is compared with Stats NZ population data to show where reports are higher or lower than expected based on regional population share. In FY26, reporting was proportionally higher in Nelson, Wellington, Auckland and Canterbury, and lower across several provincial and rural regions. The broad pattern remained stable year on year, although Auckland became more over-represented, Waikato and Gisborne moved closer to their population shares, and Southland became further under-represented.

These patterns help Netsafe understand where awareness, access or barriers to support may differ across Aotearoa, and where future outreach may be needed.

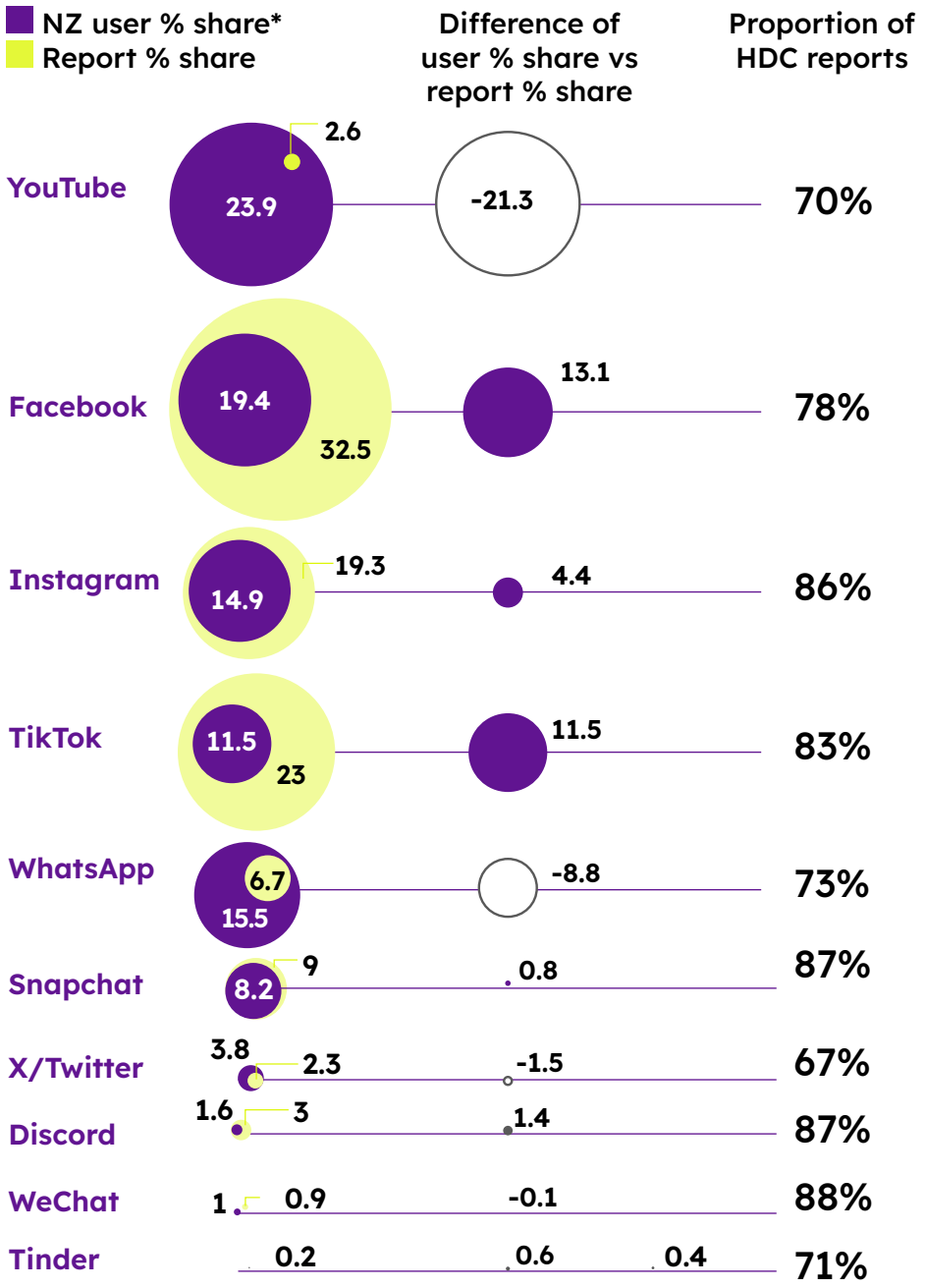


Where online harm is being reported in New Zealand

Platform reporting data helps Netsafe understand where people are seeking help online and where targeted safety advice may have the greatest value. The data compares each platform's share of reports with its estimated New Zealand audience size.

In FY26, Facebook accounted for the largest share of top-ten platform reports at 32.5%, compared with 19.4% of the combined estimated audience. TikTok was also notably over-represented and increased from 19.4% of reports in FY25 to 23.0% in FY26. Instagram, Discord, Snapchat and Tinder accounted for slightly higher shares of reports than audiences, while YouTube and WhatsApp accounted for substantially lower shares. Harmful digital communications made up a high proportion of reports across most platforms, including 87% for Snapchat and Discord, 86% for Instagram and 83% for TikTok.*

These differences are descriptive only and should not be read as showing that any platform is inherently safer or more harmful.



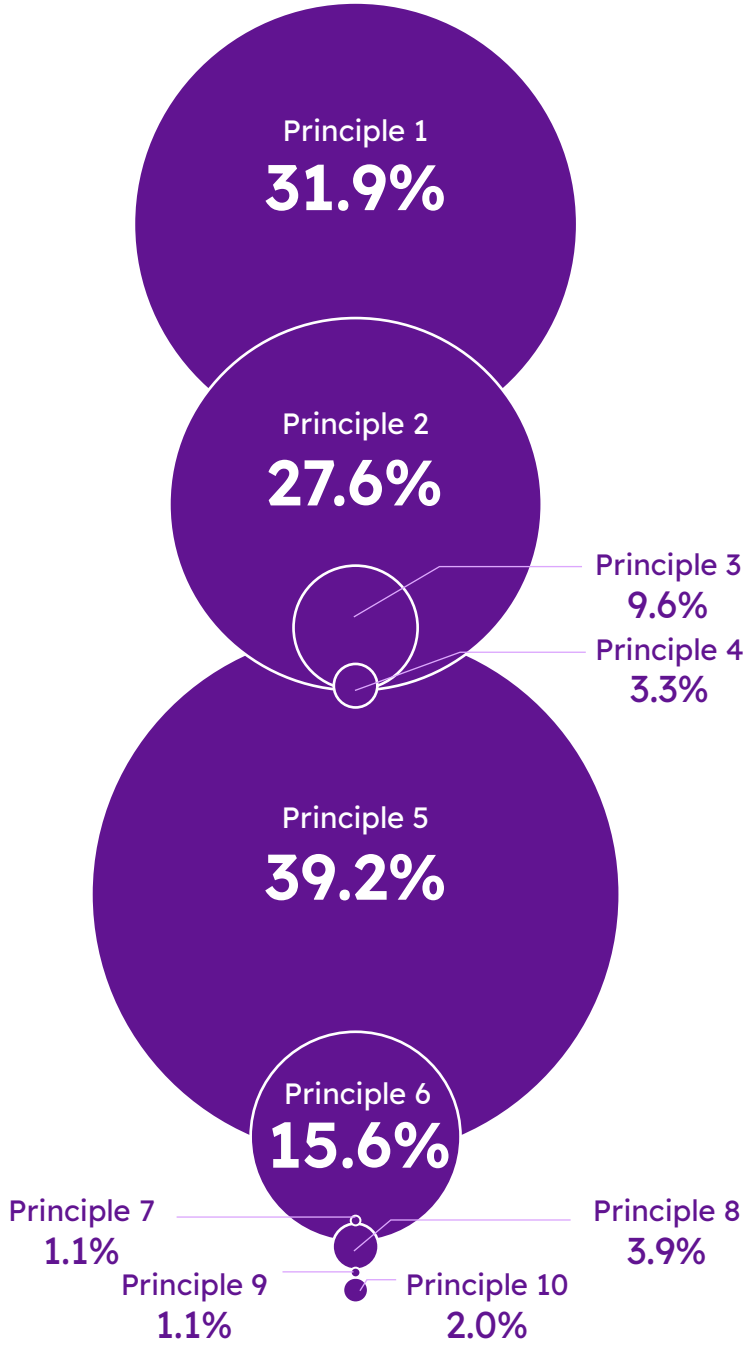
*Sources can be viewed in the Appendix on Page 45.

Complaints that Engaged One or More of the 10 Communications Principles

Under the Harmful Digital Communications Act, setting expectations for what people should not do when communicating online.

Principles		Reports*
1	A digital communication should not disclose sensitive personal facts about an individual.	2,487
2	A digital communication should not be threatening, intimidating, or menacing.	2,154
3	A digital communication should not be grossly offensive to a reasonable person in the position of the affected individual.	746
4	A digital communication should not be indecent or obscene.	257
5	A digital communication should not be used to harass an individual.	3,056
6	A digital communication should not make a false allegation.	1,214
7	A digital communication should not contain a matter that is published in breach of confidence.	83
8	A digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.	304
9	A digital communication should not incite or encourage an individual to commit suicide.	85
10	A digital communication should not denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.	159

*Reports may get counted twice as they engaged multiple principles



Reports satisfaction rate

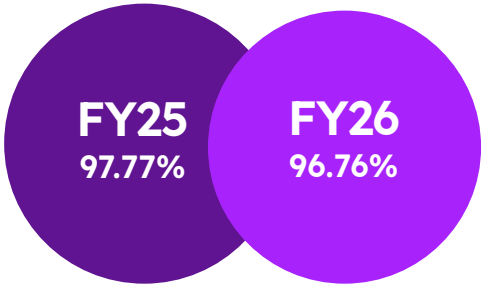
Despite unprecedented demand, Netsafe continued to provide a timely and effective service for people affected by harmful digital communications. Only 4.4% of service users requested a Netsafe Summary compared to 5% in FY25, a first step necessary to proceed with an application to the District Court.

92.13%

of HDCA complaints were resolved through Netsafe processes without needing to seek orders in the District Court in FY26.*

The average customer satisfaction rate for service users was 7.75 out of 10 and above our target of 7.5 out of 10.

Time to resolve by percentages



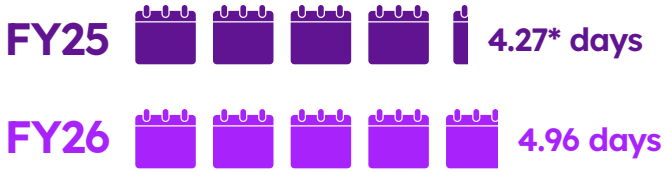
< 15 days

	FY25	FY26
< 15 days	97.77	96.76
15-29 days	2.16	3.20
> 30 days	0.06	0.04

Despite a sharp 22% increase in complaints received in FY26, Netsafe continued to provide a quick and efficient service as part of the justice system.*

These results indicate that timely resolution through Netsafe can spare many people the additional emotional, financial and administrative burden of court proceedings.

Average business days to resolve



*As the Approved Agency under the HDCA, Netsafe helps people resolve serious online harm where possible and guides them through the legal pathway when court action may be needed.
** In FY26 average business day calculations changed over the course of the year. Therefore FY25 in this report has been restated so that both years are calculated on the same basis for comparative purposes in this report as the percentages shown above. The FY25 average published in last year's review (7.4 business days) was calculated differently and is not comparable with the figures shown here.

Scams Helpline: Responding to Scams and Fraud

Scams remained one of New Zealand's most significant and fast-growing online harms. Netsafe handled 14,744 scam reports in FY26 through an essential service that continued to operate without secure, recurring and sufficient funding.

Netsafe is evolving the way it delivers scam support as scam activity continues to increase in scale, sophistication and volume across New Zealand.

Monetary loss

1,991

Scams resulted in monetary loss

$9,019,906*

Total monetary loss reported

People aged 41-64 reported the highest level of monetary loss, totaling $4.22 million NZD across 670 reports (an average of $6,291 per report).

For reports involving monetary loss, the volume of reports with female targets was 16.3% higher than males. In contrast, the average amount lost by males was 40.9% higher than that lost by females ($5,135 vs $3,645).**

Breakdown of scam reports and financial losses***

Scam Type	Total Loss
Worthless or non-existent products	**$2,596,482**
Other investment opportunities fraud	**$1,373,024**
Romance scam / sweetheart scam	**$915,274**
Friends or relatives impostor scam	**$734,386**
Work at home scam	**$419,180**
Consumer investment fraud	**$395,402**
Phishing	**$249,396**
Securities fraud	**$234,865**
Account takeover (bank or other)	**$232,858**
Unauthorised billing for products or services	**$169,831**

*In 2025 we improved the way we record total monetary loss, adding steps to verify losses, therefore comparisons to previous years can't be made.
**Number of reports received by gender diverse people reporting a scam is too small to offer accurate demographic data.

*** The categories above account for part of the $9,019,906.46 in total reported losses and should not be read as a complete reconciliation of all scam types.

Netsafe Lab: Building technology for public good

Netsafe Lab

Netsafe Lab is Netsafe's innovation and technology hub, turning frontline harm intelligence into practical tools that prevent harm, disrupt scams and extend the reach of our services.

During FY26, the Lab advanced a portfolio including ScamProof, Re:Scam V2, CheckNetsafe, an Auditor Tool for monitoring harmful-content takedowns, and interactive scam-learning resources. It also explored how AI and automation can support triage, harm management and scalable digital service delivery as demand for Netsafe's help continues to grow.

Approximately 11,000 New Zealand consumers took part in the ScamProof beta programme.



500,000+ emails sent to scammers since Re:Scam began.

ScamProof

ScamProof is designed to identify fraudulent websites impersonating trusted brands, helping people avoid scams before they provide personal information, account credentials or payment details.

During FY26, ScamProof moved from concept into large-scale beta testing. The technology assesses a range of signals, including website addresses, visual and structural similarities, brand styling and technical characteristics, and turns these into simple warnings for users.

Testing helped Netsafe refine both the detection technology and the user experience, with the product progressing towards launch. Support from Infoxchange also helped strengthen the product strategy and development process.

ScamProof is being developed as a public-good complement to commercial scam-protection products, with potential future distribution through banks, telecommunications providers, NGOs and technology companies. Its broader goal is to help people become not simply scam aware, but more scam resistant.

Re:Scam

Re:Scam continued its evolution as Netsafe's AI-powered scam-disruption platform, engaging scammers in realistic conversations that consume criminal time and resources while creating opportunities for education and threat intelligence.

During FY26, Netsafe advanced Re:Scam V2 using modern large language models, new personas, automated workflows and machine-learning moderation.

Re:Scam was also recognised internationally through the World Economic Forum MINDS programme for its human-centred use of artificial intelligence.

The platform is now evolving beyond its original scam-engagement function, with potential future roles in scam intelligence, public education, AI-powered guidance and scam disruption. Netsafe also explored a honeypot extension aimed at disrupting romance scams.

Re:Scam recognised as one of 30 global projects in the World Economic Forum MINDS programme.

Building an innovation portfolio

ScamProof and Re:Scam sit within a wider Labs portfolio designed to turn online safety expertise into practical interventions.

During the year, the Lab also led or supported CheckNetsafe, interactive scam-learning resources and a tool designed to monitor harmful-content takedowns.

Together, this work shows how Netsafe can use technology to prevent harm earlier, strengthen digital capability, disrupt offending and deliver services at greater scale.

Netsafe Lab is becoming an increasingly important part of Netsafe's future. By combining trusted online safety expertise with responsible technology, it is creating products and services that extend our reach and strengthen the wider online safety system.



Protecting Children against Child Sexual Abuse Material (CSAM)

Netsafe is New Zealand's member of INHOPE, the international network of more than 50 hotlines working to combat child sexual abuse material (CSAM) online. The network enables reports of CSAM to be shared quickly between countries so they can be referred to the agencies best placed to act.

The value of this international network is reflected in the speed with which material can be addressed. **The average takedown time for CSAM hosted in a country with an INHOPE hotline is 2.5 days, compared with 28 days in countries without a hotline.** This materially shortens the time illegal material may remain accessible and reduces risk of continued victimisation.

Netsafe receives CSAM reports through two distinct channels. Reports are received through ICCAM, INHOPE's international case management system, where material identified by analysts within the network as illegal and linked to New Zealand is referred to Netsafe. We also receive reports directly from members of the public in New Zealand and overseas about suspected CSAM.

Reports received by Netsafe are assessed and referred according to where the material is hosted and which agency is best placed to respond. This means referral to the appropriate New Zealand law enforcement or regulatory agency, or referral through the INHOPE network or to an appropriate international agency for action.

In FY26, Netsafe received and processed 1047** reports relating to suspected or confirmed CSAM through these two reporting channels:

- 503 reports were received through ICCAM and referred to the appropriate law enforcement or regulatory agencies in New Zealand.
- 544 reports were made directly to Netsafe by members of the public. These were assessed and, where appropriate, referred to New Zealand law enforcement or regulatory agencies, through the INHOPE network, or to relevant international agencies.

These figures represent reports received and processed by Netsafe. They do not represent the number of individual images, victims or offenders. The two reporting channels describe how reports reached Netsafe, rather than different categories of outcome.



544 + 503 = 1047

Netsafe Reports	ICCAM Reports	Total CSAM Reports In FY26

*ICCAM operational numbers

**503 reports were classified as illegal by analysts at organisations that are members of the INHOPE network (ICCAM). 544 additional reports were made directly to Netsafe by the public for a total of 1047 CSAM related reports.

Recognised for Service Excellence

Independent recognition matters because people often contact Netsafe in distress or moments of uncertainty. These awards provide external assurance that the service they receive is operationally keeping up with best practices.

For a third year in a row, Netsafe was independently assessed as a leading contact centre in New Zealand. At the NZ CRM Contact Centre of the Year awards, Netsafe received five awards:

- Most Outstanding Customer Service Representative
- Excellence in Learning from AI Projects
- Online Support Services – Industry Category Winner
- Outbound Business-to-Consumer – Gold Award Customer Care
- Supreme Award – Gold Award Contact Centre under 50 Seats



Education: Supporting Safer Schools & Kura

In schools, Netsafe continued to support digital citizenship education through the Kete platform and direct consultation with teachers and school leadership teams.

Adding to the platform of resources for schools and their communities, we developed on-demand videos for supporting young people through online incidents, a cyberbullying prevention toolkit across year levels, and expanded guidance for schools responding to complex online harm.

Insights from educators and young people helped ensure resources remained relevant.



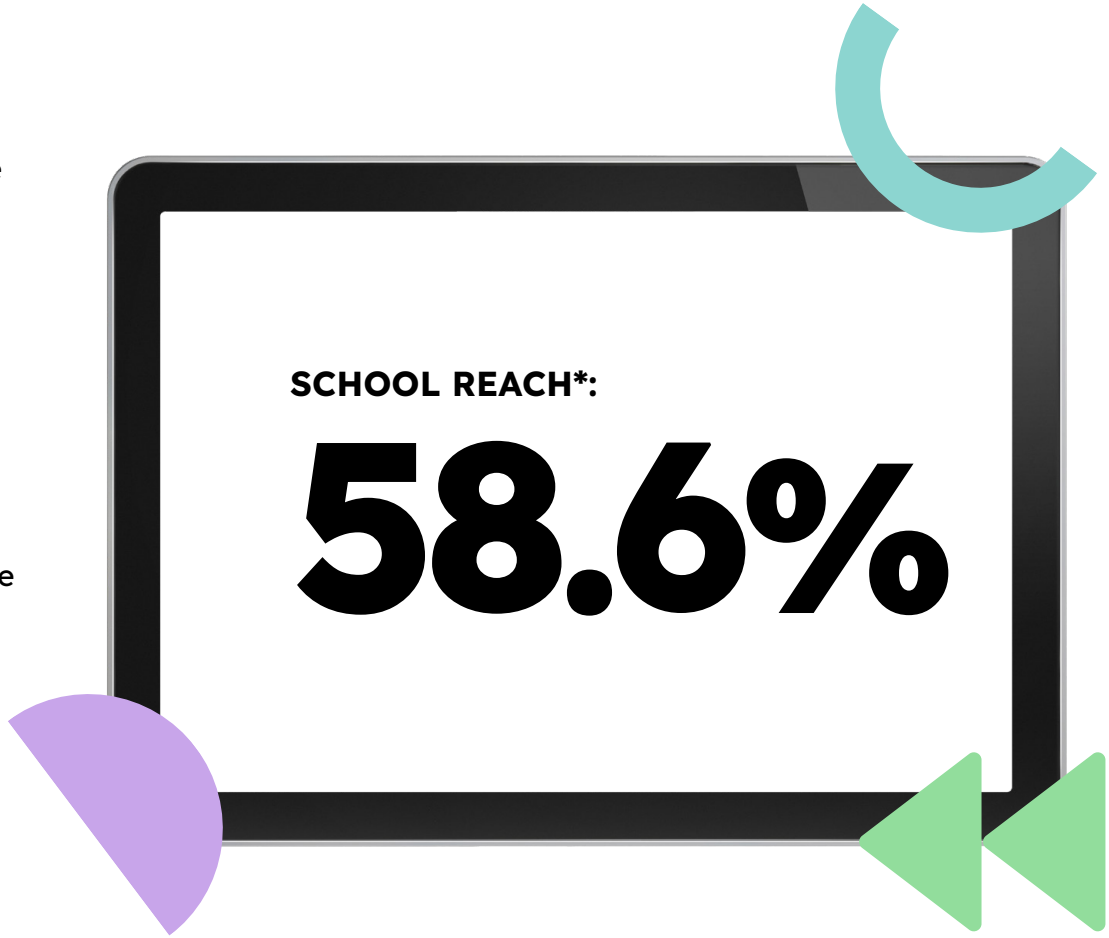
> “Netsafe Micro Learns help us to engage students on a new level. It allows us to feel like we can talk to them about the things that are important in their world.”
>
> TEACHER, AUCKLAND

Kete Platform

The Kete education platform continued to grow as a central source of online safety support for schools and educators. During the year, we upgraded the Kete platform, increasing the visibility of content and resources and improving the user experience. We also established the Kete Advisory Group, bringing together frontline educators to co-design, test and continuously improve Netsafe's curriculum aligned education resources.

The figures show that Kete is not only a repository of resources, but a national support channel, reaching more than half of New Zealand schools and supporting educators and students with online safety learning at scale.

Our next step is to strengthen outcome measurements so we can demonstrate not only how many people used these resources but whether they feel more confident, changed behaviour, or responded more effectively to online harm.



17,076 **MICROLEARN SESSIONS COMPLETED BY 10,210 USERS**

building practical online safety knowledge through short lessons that take only a few minutes to complete

6,530

KETE REGISTERED ACCOUNTS

31,717

KETE RESOURCE DOWNLOADS

used in classrooms as part of teacher lesson plans

*School Reach: 1,503 out of 2,565 schools.

Young people shaping online safety

Our newly recruited Youth Action Squad brought together 10 high-school-aged students from across Aotearoa to lead youth-led action on online safety and wellbeing. At their first hui, members explored young people's digital experiences and, with Netsafe's support, helped shape a national survey for students in Years 7–13. More than 800 responses are now informing YAS priorities and the development of new learning materials created with young people, not just about them.

YAS gained further momentum through Netsafety Week, where it was showcased in a national rangatahi webinar, and through continued use of the youth-designed toolkit to help schools establish their own squads. We also recruited a new national cohort for 2026.

A three-year grant from Otago Community Trust will extend this youth-led approach by establishing regional young digital-leader groups across Otago.

Together, this work is growing a network of young people actively shaping how Netsafe and schools respond to the digital experiences that matter to them.



"We are encouraged to give our young people credit; they are getting better at being online. We as educators are helping… but we couldn't do it without Netsafe." INTERMEDIATE SCHOOL, CANTERBURY

Public Education: Harm Prevention in Partnership

Embedding online safety into services and tools for families

Netsafe's education work helps people recognise risk earlier, take safer action and know where to turn before online harm becomes a crisis.

Launched in May, The Digital Guardian Guide, supported by Spark Foundation, The Lion Foundation, Four Winds Foundation and Trillian Trust gave parents, caregivers and whānau practical support to navigate children's online lives, attracting 34,039 unique users and 54,691 sessions. Users rated it 4.4 out of 5, valuing its clear, practical guidance for starting conversations, recognising risks and making informed decisions.

Netsafe worked with Spark to extend trusted online-safety guidance to families as children begin using connected devices. In FY26, Spark launched New Zealand's first child-focused mobile plan, combining parent-managed data with protections against marketing messages, premium texts and unexpected purchases. By embedding Netsafe guidance and referral pathways into Spark's parent and caregiver support, the partnership helped families access practical advice earlier — from parental controls and privacy to screen-time boundaries and reporting options when something goes wrong.

"From my point of view, Netsafe is essential in Aotearoa because feeling safe online is what enables people to actually participate in the digital world. Access to devices or connectivity means very little if people are scared, unsure, or don't know where to go when something goes wrong." NATALIE LAWSON, CHORUS SOCIAL IMPACT LEAD



54,691
sessions

Free online resource for whānau

"We've been really impressed with the Digital Guardians Guide and the value it is already creating for families and communities. It is a strong example of a practical, community-focused solution that helps people build the confidence and skills needed to participate safely in an increasingly digital world. We see significant potential for the Guide to increase both its reach and impact as you continue to develop, promote, and strengthen the resource over the next two years." ROBYN BISSETT, DIGITAL EQUITY PARTNER (COMMUNITY & PARTNERSHIPS) SPARK FOUNDATION

Building young people's digital resilience

We also continued to build young people's digital resilience through Headspace Invaders, an interactive resource helping 12–16-year-olds recognise and respond to harmful or manipulative online content. Introduced at a Parliament event and developed in conjunction with Dr Helen Sissons, Dr Philippa Smith and Distinguished Professor Emeritus Paul Spoonley ONZM, it engaged more than 56,000 active users and recorded 267,000 interactions, supporting early intervention across misinformation, disinformation, hate speech and online extremism.

Making online safety support more accessible

Partnerships helped reduce barriers to trusted advice for communities less likely to access mainstream online-safety information. With support from Chorus, this included resources for older adults through Get Set Up for Safety, to support practical conversations about scams, privacy and staying safer online. We also released materials in Pacific languages and Traditional and Simplified Chinese to make online safety information more accessible to more communities. We also developed the Hōhepa Digi Citizens toolkit with Hōhepa North Canterbury, supporting people with intellectual disabilities to build digital confidence and safety skills.



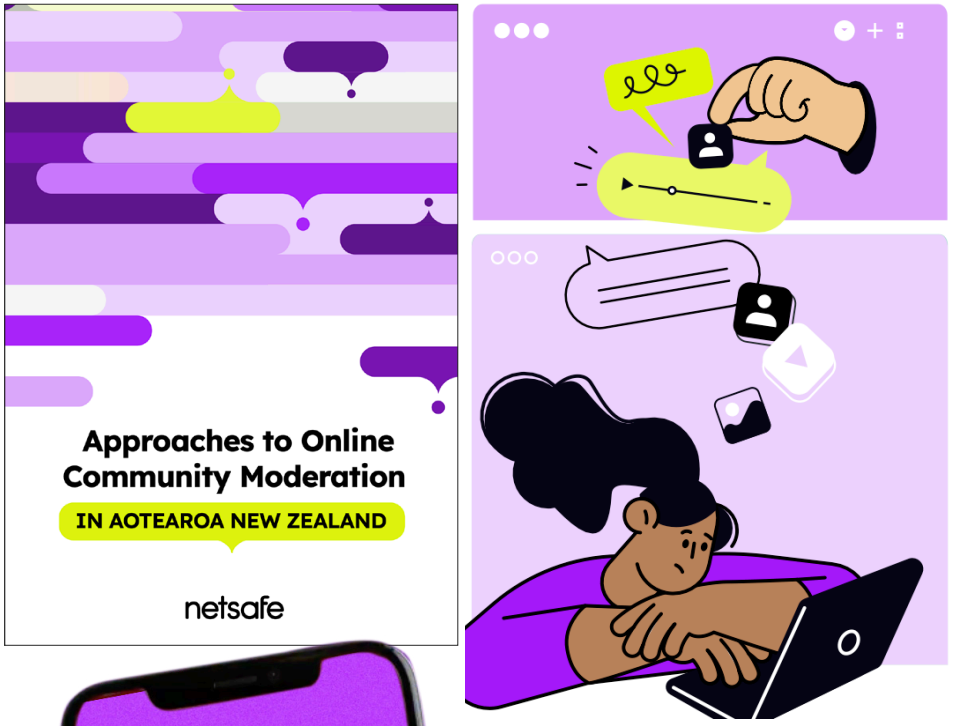
"We sponsored Netsafe's Get Set Up for Safety initiative and later used those resources at the Digital Seniors Tech Expo. Having trusted Netsafe materials available helped us engage seniors in practical conversations about online safety, which then led into broader discussions about how they stay connected, including device access and internet connectivity." NATALIE LAWSON, CHORUS SOCIAL IMPACT LEAD

Helping communities to prevent, and respond to online harm

Netsafe also turned research and frontline evidence into practical prevention tools.

We developed Approaches to Online Community Moderation in Aotearoa New Zealand, practical guidance to support administrators and moderators of social media groups, pages and forums to manage online spaces more safely and consistently.

> “I was very pleased to see how it was translated into something that is extremely useful for a wide range of moderators who come from all backgrounds.”
>
> DR. PHILIPPA SMITH, INDEPENDENT RESEARCHER AND DIGITAL CONSULTANT, P K SMITH PROFESSIONAL



Good to Know Campaign

Campaigns and public events extended this prevention impact. The Good to Know campaign helped more New Zealanders understand when Netsafe can provide advice and support. Running across search and social media during February and March, it reached more than one million people, generated 6.3 million impressions and drove 31,389 visits to practical online-safety information.



Netsafety Week 2025

Netsafety Week 2025 demonstrated the “Power in Partnerships”, by mobilising educators, libraries, young people and community organisations with more than 65 libraries participating nationwide, extending support to older people, teenagers and te reo Māori audiences across the motu. Four webinars and a specialist e-sports session translated expertise on AI, rangatahi experiences, indigenous perspectives and safer gaming into practical guidance.

ALReR Conference Partnership

Netsafe partnered with The University of Auckland’s Centre for Advancing Law and Technology Responsibly (ALTeR) as a sponsor and workshop organiser of their inaugural conference. Our workshop connected debate about AI-enabled harm, accountability, regulation and education with evidence from people seeking frontline support. We also supported Child Safeguarding Week, Safer Internet Day with advice on emerging risks such as sextortion and scams, helping people recognise warning signs and take action earlier.

Together, this work shows Netsafe’s prevention impact: helping people build confidence, recognise harm sooner, access trusted support faster and participate online with greater safety and trust.

“The Netsafe resources are great, we are still handing out the Get Set Up For Safety resources, they are so handy. I just did the quiz with a group of Kaumātua today!” **LEALA FALESEUGA, DIGITAL INCLUSION COORDINATOR, LIBRARIES HOROWHENUA**

Women, girls and gendered online harm

Online abuse does more than harm individuals. It can silence women, constrain participation and deter future generations from entering public and leadership roles.

Netsafe provided prevention, support, evidence and advocacy addressing gendered online harm. Through our ongoing partnership with Women’s Refuge, Shine and The Light Project, we created guidance to help people recognise technology-facilitated coercive control, take safer steps and connect with specialist support. We also worked with the same group, plus Auckland Women’s Centre, to develop advice on technology-facilitated stalking, providing clear information about recognising stalking behaviours, staying safer online and accessing appropriate support.

We developed Netsafe guidance on online misogyny and the manosphere, helping parents, whānau and educators understand how harmful gender narratives can develop and spread through online communities.

Kia noho haumaru, kia kaha.

Stay safe, stay strong.



Public Education Highlights

317,648

NETSAFE.ORG.NZ ACTIVE USERS FY26



Netsafe's website performance

743,588

PAGE VIEWS

2.34

PAGE VIEWS PER ACTIVE USER

1m 24s

AVERAGE ENGAGEMENT TIME PER ACTIVE USER

Top topics

1. **UNDERSTANDING AND AVOIDING SCAMS** (24,671)
2. **SCAMS** (16,415)
3. **HARMFUL DIGITAL COMMUNI-CATIONS ACT** (13,452)
4. **UNDERSTANDING SEXTORTION EMAIL SCAMS** (12,012)
5. **FACEBOOK MARKETPLACE SCAMS - LEARN TO SPOT THEM & GET HELP** (11,888)

Turning Research Evidence into Actions

Netsafe conducts, commissions and invests in independent research that strengthens New Zealand's understanding of online harm, digital participation and social cohesion. During FY26, this evidence informed public debate, policy submissions, education resources, service design and national conversations about the systems shaping people's digital lives.

Social Cohesion in New Zealand 2026

As one of the study's funding partners, Netsafe helped make possible the Helen Clark Foundation's second annual national study of social cohesion. Based on a survey of 2,882 New Zealand adults, including representative booster samples for Māori, Pacific and Asian communities, the research examined belonging, trust, participation, isolation and the forces shaping New Zealand's social fabric.

A new social-media module, which Netsafe helped shape, found that 54% of New Zealanders believe social media is bad for society, despite 56% using it several times a day. The study also found that people with more diverse news diets reported stronger social-cohesion outcomes, reinforcing the importance of media literacy, access to trustworthy information and healthier online environments.

Netsafe's support extended the evidence base connecting digital participation, social isolation, institutional trust and social cohesion. The findings informed national discussion about how online environments can either deepen division or strengthen belonging and democratic participation.

54% of New Zealanders

believe social media is bad for society —yet 56% use it several times a day.

Understanding recovery after cyber sextortion

Netsafe supported New Zealand participant recruitment for a Monash University study examining vulnerability and recovery following cyber abuse and sextortion. The ethics-approved qualitative research explores how victims regain identity, agency, safety and belonging, and what roles personal resilience, relationships, legal pathways and support services play in recovery.

By helping include experiences from Aotearoa New Zealand, Netsafe contributed to research intended to improve understanding of different recovery trajectories and inform the future development of a measure of post-traumatic growth. Practice-relevant findings will be shared with Netsafe to support future services, training, advocacy and policy work in the area of sextortion.

Rise in sextortion and extortion targeting New Zealanders

Netsafe Sextortion Survey Insights Report July 2025

21% of NZ adults had direct or indirect experiences of sextortion incidents, with 35% of victims reporting the impact on their mental wellbeing was moderate to severe.

These findings are already driving change: they shaped our sextortion website and summer awareness campaign, helped establish partnerships with Indian counterparts, and supported our Proceeds of Crime application for a multi-year national campaign.

Young people's insights into online safety

Digital Resilience Research Report 2025-2026

Beyond a Single Story: Understanding Young People's Digital Experiences

61% of the 174 young people described connection as a key part of what they get out of being online.

"Youth are not just the future. We are the now. Youth need to be more involved especially in decisions that involve us."

These insights were used for Netsafe's submissions to Parliament on various bills and to inform youth programmes in Otago and for our Youth Action Squad service design.



$3b

stolen by scammers in NZ in the last year

The growing impact of scam losses

State of Scams in New Zealand 2025 Report

72% of adults encountered a scam in the last 12 months, pushing national losses to around NZ$3 billion.

Netsafe used this data in our media commentary, outreach to communities and engagement with global anti-scam alliance partners.

Long-term changes in attitudes to and the nature of online harm

Netsafe 2025 Annual Population Survey: Māori Population Report

48% of Māori have received unwanted digital communications in the past year with 52% of recipients saying these communications have had a negative impact on their life - up from 39% in 2023.

This research gives Netsafe an evidence base for its policy advice, prevention priorities and service design. It allows us to track changes in online harms and public attitudes over time and to identify emerging risks and differences between population groups.

Media for online safety messages

Netsafe became a more visible voice in the national conversation about online harm. Between 12 July 2025 and 30 June 2026, we received 1,339 media mentions—53% more than the previous year—with average monthly coverage rising from 72 to 112 mentions. Online news generated the greatest reach, alongside 77 radio and 18 television appearances.

An innovation was the introduction of regular scam intelligence releases, turning frontline reports into timely public warnings about emerging and seasonal threats. This enabled Netsafe to alert New Zealanders as tactics changed—from sextortion and impersonation to tax-refund scams—and provide clear steps people could take to protect themselves.

Original research and frontline evidence generated some of the year's strongest coverage. Netsafe exposed the estimated $3 billion national cost of scams, record demand under the Harmful Digital Communications Act and the rapid growth of AI-enabled abuse, including deepfakes and fake intimate images. These findings gave journalists evidence behind individual experiences, strengthened calls for law reform and positioned Netsafe as a source for independent online safety intelligence.

53% increase

on FY25 media coverage



1,339

media mentions

Reaching Communities Where They Are

Netsafe's community engagement focused on reducing barriers to trusted online-safety information, particularly for communities less likely to encounter our services online and through mainstream channels.

We had a focus on Māori, Rainbow, and Pasifika communities this year. This involved connecting with Māori whānau at Waitangi and sharing our te reo Māori resources. We marched for a second time in the Rainbow Parade, alongside community partners, showing our support for LGBTIQA+ communities and delivering online harm prevention messages that promoted safer, more inclusive online spaces.

In March 2026 at the Pasifika Festival, we connected with communities and shared online safety information and resources in a range of languages and took enquiries face to face about online harm incidents. The event built trusted relationships and created a network of individuals willing to join a community of practice and improve access to culturally relevant online safety information.

Insights and relationships developed through these events are informing sustained, community-led outreach rather than one-off engagement.

Many people we have met have become Netsafe members, and we are now working with organisations on grant applications and consortium-led harm-minimisation projects, including a tool for Rainbow communities and co-designed workforce development training supported through the Mental Health Innovation Fund.



Māori Leadership Shaping Online Safety and Digital Guardianship

This year, Netsafe continued to strengthen its commitment to working alongside Māori to shape safer, fairer and more trusted digital environments.

A central focus was the Māori Online Harm Ecosystem kaupapa, led through the Iwi Leaders Group Online Safety Pou and supported by the Ministry of Justice.

This work moved beyond examining individual forms of online harm to consider the wider systems in which harm occurs, including platform design, artificial intelligence, commercial incentives, misinformation, data use and gaps in governance.

Through hui and engagement with iwi, whānau and rangatahi, the kaupapa created space for Māori experiences and aspirations to inform the future of online safety.

In May 2026, Netsafe supported a Mana Online hui in Huntly, focused on raising awareness and improving online safety for rangatahi. The event provided an opportunity to connect directly with rangatahi and promote our resources and services.

The year also saw the development of a broader framework of digital guardianship, led by Amokura Panoho, Netsafe's Poutaki Mātauranga Māori. Drawing on mātauranga Māori, whakapapa and kaitiakitanga, this work asks not only how we support people after online harm occurs, but how Māori can help shape the digital environments, technologies and systems that affect whānau in the first place.

This will now guide Netsafe's approach to services, research proposals and engagement with Māori.

As artificial intelligence and digital systems become more deeply embedded in everyday life, Netsafe will continue working alongside Māori to ensure that technological change strengthens mana, relationships and collective wellbeing.



Amokura Panoho, Netsafe's Poutaki Mātauranga Māori

Global Ideas, Engagement and Impact

In FY26, we shared our expertise with international audiences regarding online safety, scam prevention and digital harm response initiatives.

We contributed to the development of the United Nations Public-Private Partnership Toolkit Against Organised Fraud, which recommends a global framework to strengthen collaboration between governments, industry and civil society. Through this work, Netsafe shared expertise on fraud prevention, victim support and coordinated responses to organised fraud.

Netsafe grew closer ties with India through a bilateral travel exchange supported by the Asia New Zealand Foundation. The visit linked us with diplomatic, legal, media and policy communities and led to joint funding applications, discussion about foreign student online safety and capability building between helplines. It led to a new Memorandum of Understanding with Social Media Matters, an India-based organisation working at the intersection of technology, human rights and social change, to share knowledge and build mutual capability. With further support from the Asia Foundation, Netsafe delivered a panel on Reducing AI-driven Digital Harms for Minors: Platform Accountability, Age Assurance and Safety by design at the India AI Impact Summit. This shaped conversations on child online safety and responsible AI and safeguards to lay the foundation for partnerships and capability-building work now underway.

During the year, we successfully established and led the Oceania chapter of the Global Anti-Scam Alliance as its founding Chair for 18 months. We then supported the successful transition of leadership to the Global Anti-Scam Alliance, ensuring the chapter was well positioned for its next phase of growth.



Welcoming international education delegations

Netsafe hosted community and education connections as part of international delegations from China and the Republic of Korea. In March 2026, Netsafe welcomed 20 Chinese educators as part of the China-New Zealand Anti-Bullying and Wellbeing Education Exchange Programme, sharing approaches to digital citizenship, online safety, student wellbeing and harm prevention. Feedback from the exchange highlighted potential for collaboration between New Zealand and Chinese educators. This also led to relationship development with technology companies and academic organisations in the Haidian and Zhongguancun innovation districts in Beijing.

For a second year running we hosted a similar sized Korean delegation in April 2026, which created opportunities for knowledge sharing about ways to deliver online safety education messages to youth and the development of digital safety and digital citizenship policy positions for school communities.

Trans-Tasman collaboration and regional impact

Working alongside Australian government-funded digital safety programmes, regional anti-scam initiatives, digital safety programme, platform engagement and civil society organisations, we contributed expertise to initiatives across Australia, Papua New Guinea and the wider Pacific region. Engagements with Meta, Google, Apple, Snapchat, Interactive Games and Entertainment Association and specialist services addressing family violence helped build our capabilities, develop content, technical guidance, reporting pathways and policy approaches to digital safety.

Strengthening online safety across Association of Southeast Asian Nations (ASEAN)

Netsafe built its relationships and influence across ASEAN during the year, positioning our New Zealand expertise in online safety, scams, violent extremism and responsible technology within regional policy and capability-building networks.



In Malaysia, our work with the Southeast Asia Regional Centre for Counter-Terrorism helped deepen regional capability around preventing online radicalisation and violent extremism, while reinforcing the importance of balancing harm prevention with freedom of expression and other human rights. Engagement with the Centre for Independent Journalism, Sinar Project and ARTICLE 19 also broadened our regional civil-society partnerships and created stronger pathways for future joint research, training and policy work.

Across Singapore and Indonesia, we used our growing regional networks to connect practical harm-response experience with emerging challenges in scams, fraud and AI governance. Through the Global Anti-Scam Alliance, TrustCon, Bank of Indonesia and UNESCO, we contributed New Zealand experience to regional discussions on disrupting fraud networks, strengthening institutional responses and building capability for responsible AI governance.

Importantly, some of these engagements were repeat invitations from countries, moving Netsafe beyond one-off participation towards a stronger ASEAN platform for future collaboration and strengthening our position as a trusted Asia-Pacific partner, able to translate frontline online-safety experience into practical regional helpline, education and tech-for-good solutions.

The next step is to build on these relationships through funded training, research and capability-building that strengthen regional responses to online harms across borders.

Building locally led Pacific online safety capabilities, where support is limited

Our long-term goal is to support locally owned capability, enabling Pacific partners to respond confidently and sustainably.

Confident and connected Pacific Island nations

Netsafe continued to build online safety capability across the Pacific. Supported by the APNIC Foundation's Information Society Innovation Fund (ISIF Asia), we delivered the Confident & Connected regional train-the-trainer programme across the Cook Islands, Tonga and Fiji. Working with the Online Safety Commission Fiji, Fiji National University, CERT Tonga, Tonga Women in ICT and the Centre of Excellence in Information Technology in the Cook Islands, the programme equipped local facilitators to support older people to recognise scams, protect their privacy, use digital devices safely and build confidence online.

Twenty-two facilitators were trained across the region, strengthening local capability to deliver Confident & Connected within their own communities.



"Working together is wonderful - especially to us who are usually left behind. We are old, and from baby boomers, but you know we are still here - we have skills before the AI. Because we don't know AI and the internet - but we have other knowledge from years of experiences. So thank you all for everything and hope to see you again to help us, to upgrade us." PARTICIPANT, TONGA WORKSHOP

Building safe and productive digital participation in Vanuatu

After two years of partnership development, Netsafe supported the launch of Vanuatu's first Economic Micro-Hub, Emua Vila, in North Efate in April 2026. Led locally by the Government of Vanuatu and the North Efate community, the initiative brings connectivity, government services, digital learning, business support and access to markets closer to rural communities.

Netsafe contributed specialist online-safety education, helping ensure that expanded internet access was accompanied by the knowledge and confidence needed to participate safely. At pre-launch community workshops, Netsafe and other partners introduced residents and local administrators to the services and opportunities available through the hub, including online-safety learning, digital skills, business mentorship and access to digital markets.

The hub serves five Area Councils—North Efate, East Efate, West Efate, Nguna-Pele and Emau-Takara—and supports local businesses, farmers, women, young people and entrepreneurs to access information, services and economic opportunities closer to home. Its cost-recovery and community-ownership model is designed to support long-term sustainability rather than short-term access alone.

The initiative brought together the Government of Vanuatu, community leaders, Welchman Keen, Netsafe, Samsung New Zealand, Digicel Vanuatu and CEO.com. Its official opening by Prime Minister Jotham Napat reflected national support for a model connecting digital inclusion with economic empowerment, decentralised services and safer online participation.



Turning shared expertise into local action in Papua New Guinea

We also supported Papua New Guinea's 1-Tok Kaunselin Helpim Lain gender-based violence helpline by sharing expertise in online harm response, service delivery and operational best practice.

Our Pacific work also helped strengthen Papua New Guinea's response to technology-facilitated gender-based violence, including supporting its first successful harmful content takedown requests. This practical support helped turn shared expertise into tangible outcomes for people experiencing online harm and strengthened regional capability to respond to similar cases in future.

Influence, Advocacy and Systems Change

Helping shape the implementation of New Zealand's first standalone stalking offence

New Zealand's new stalking offence was established through the **Crimes Legislation (Stalking and Harassment) Amendment Act 2025**, which came into force on 26 May 2026.

The reforms created links between the new stalking offence and the Harmful Digital Communications Act (HDCA), marking a significant development in New Zealand's response to technology-facilitated abuse, harassment and stalking. The District Court now has additional opportunities to make HDCA-related orders in stalking cases.

Netsafe worked alongside the Ministry of Justice and New Zealand Police to support implementation of the new legislation and help ensure victim-survivors could access appropriate information, support and pathways to safety. In partnership with Women's Refuge, Shine and The Light Project, Netsafe developed practical guidance on technology-facilitated online stalking, including how to recognise stalking behaviours, stay safer online and access specialist support.

Netsafe also advised on victim pathways, public guidance and the interaction between the new offence and the HDCA. Together with the practical guidance developed with Women's Refuge, Shine and The Light Project, this advice helped connect legislative implementation with clear information and support for victim-survivors. The work was undertaken without additional implementation funding and reflects Netsafe's ongoing commitment to strengthening New Zealand's justice response to online harm through collaboration and victim-centred approaches.



Strengthening protections from gendered and AI-enabled harm

Netsafe used frontline evidence, research and policy expertise to advocate for stronger protections from gendered online harm, including technology-facilitated abuse, stalking and AI-generated intimate-image abuse.

In June, Netsafe supported stronger legal protection through our submission on the Deepfake Digital Harm and Exploitation Bill. Drawing on frontline cases, we argued that victims should receive the same protection whether an intimate image is authentic, altered or entirely synthetic. Reports to Netsafe involving deepfakes and synthetic media had more than doubled, with women and girls disproportionately affected by sexualised deepfakes.

Netsafe's data, research and policy positions also informed the Ministry for Women's Free to Lead Long-term Insights Briefing, tabled in Parliament in June 2026. The briefing examined how online harm can silence women, damage careers and discourage girls and young women from pursuing leadership. This work built on the Free to Lead toolkit developed by Netsafe and the Ministry for Women, connecting practical support for women and employers with a growing national evidence base for systemic change.

Submissions and public policy

Netsafe used evidence from 27,482 helpline reports, national research, frontline casework and decades of online-safety expertise to advocate for laws and policies that reflect how online harm is experienced.

Netsafe's advocacy contributed to tangible policy progress during the year. The Education and Workforce Committee's final report on online harm reflected several positions advanced in Netsafe's submission, including modernising the Harmful Digital Communications Act, strengthening platform accountability and safety-by-design, investing in parent and youth education, supporting New Zealand-based research and improving coordination across the online-safety system. The Committee also cited Netsafe's research and recommended Netsafe resources to young people, parents and caregivers.

Parliament also progressed deepfake legislation consistent with a reform Netsafe had advocated for since 2021: ensuring people receive the same protection whether intimate imagery is authentic, manipulated or entirely synthetic. Our 2026 submission supported the Bill and proposed a targeted amendment to prevent synthetic imagery receiving narrower protection under the HDCA. The Bill remained before the Social Services and Community Committee at year end, so the outcome of that recommendation was still pending.

Our critical-infrastructure submission brought a public-facing harm perspective to a process primarily focused on technical security. It called for scams, social engineering, user harm and public trust to be recognised as infrastructure risks, and for frontline harm intelligence and victim-support pathways to form part of national resilience planning. The Government confirmed that submissions would inform further analysis and advice to Cabinet; no final policy decisions had been published by year end.

DURING FY26, NETSAFE MADE SUBMISSIONS ON THE FOLLOWING MATTERS:

30 July 2025
Netsafe submission to Parliamentary inquiry into online harms encountered by young New Zealanders.
Read more here.

19 April 2026
Netsafe submission on Strengthening the Cyber Security of Critical Infrastructure in New Zealand.
Read more here.

17 June 2026
Netsafe submission on the Deepfake Digital Harm and Exploitation Bill.
Read more here.

Our Priorities for the Year Ahead

Shaping New Zealand's Digital Future

For 28 years, Netsafe has helped New Zealanders navigate the opportunities and challenges of the digital world. As technology continues to transform every aspect of our lives, its role is evolving too.

AI, increasingly sophisticated scams, online exploitation, financial crime, misinformation and rapidly changing digital platforms are reshaping the nature of online harm. These challenges cannot be solved by any one organisation, sector or technology alone. They require a coordinated national response built on trust, evidence, innovation and shared responsibility.

Over the coming year, the focus will be on three priorities that will help create a safer, more trusted and digitally confident New Zealand.

1

Building a digitally confident and resilient New Zealand

Prevention starts with confidence: helping people recognise risk earlier, make safer choices and know where to turn when harm occurs. Netsafe will continue strengthening practical education, resources and community partnerships so children, young people, whānau, educators, older adults and communities can participate online with greater safety and trust.

2

Leading a stronger digital safety system

Online safety is a team sport. Online safety requires shared responsibility across government, industry, iwi, education, financial services, telecommunications, community organisations and civil society. Netsafe will continue using frontline evidence, research and partnerships to inform policy, improve practice, support stronger platform accountability and help shape a system where safety is designed in, not added on.



3

Delivering trusted support while preparing for what's next

People experiencing online harm need timely, practical and compassionate support. The goal is to ensure Netsafe is New Zealand's recognised No Wrong Door for online harm, connecting immediate support with specialist services, prevention and system-level change. We will continue protecting the services New Zealanders rely on today while investing in innovation, evidence and new ways of working to respond to AI-enabled harm, scams, exploitation, misinformation and other rapidly evolving risks.

Looking ahead

Technology will continue to change, but Netsafe's purpose remains constant: helping New Zealanders participate in the digital world with greater confidence, safety and trust. A safer digital future cannot be delivered by one organisation alone. It is something we build together.

As debate about youth online safety intensifies, future approaches will need to balance stronger protections for young people with practical, evidence-based strategies, including: greater platform accountability, safer feeds, stronger duties of care, and digital citizenship and literacy.

Netsafe is also undertaking a 24-month transformation approach focused on organisational impact, AI experimentation, strategic positioning, revenue diversification and service redesign to ensure greater capacity to respond to emerging online harms.

Legislation and Compliance

We are committed to protecting the integrity of our service.

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

The table records the requests for information (RFI) under the Official Information Act 1982 and the Privacy Act 2020. Netsafe will refuse requests or withhold information in accordance with the legislation, for example, where they believe the disclosure would involve the unwarranted disclosure of another person's affairs. This can be the case where an author of an alleged harmful digital communication requests information provided to Netsafe by the person who has been the target of the communication. When they do refuse, requesters can exercise their right to complain to the Privacy Commissioner or the Ombudsman about the decision.

Year	FY26	FY25
RFI requests received	85	66
Withdrawn requests	1	6
RFI timeframe met	84	60
Complaints to OPC or Ombudsman	0	1

Financial Performance

Netsafe's financial statements were audited by Nexia Audit Christchurch. Outlined below is a summary of Netsafe's financial highlights. All figures provided are excluding GST.

Revenue

For the 12 months from 1 July 2025 to 30 June 2026, Netsafe's total revenue excluding finance income was $7,369,240. Income generated was $511,904 less than the budget of $7,881,144, but more than last year's $6,888,763. During the year, Netsafe refined its approach to the classification of exchange and non-exchange revenue to better align with current accounting standards and financial reporting practices. This has resulted in changes to how certain revenue streams are presented in the financial statements.

Expenditure

The total expenditure for the 2025/2026 financial year was $7,462,086.

Surplus/Deficit

Netsafe ended the financial year with a net deficit of $90,593, reflecting Netsafe's ongoing strategic investment in people, technology and infrastructure to strengthen organisational capability, resilience and long-term sustainability. The financial result was also influenced by the timing of funding, with several grants and partnership contributions expected to be recognised in the following financial year.

While this represents a further year of operating at a deficit, the result was anticipated and carefully managed, reflecting deliberate decisions to invest in Netsafe's future and ensure the organisation remains well positioned to deliver meaningful impact in the years ahead.

How our work is funded

Netsafe uses a whole-of-society funding model that brings together government, philanthropy, industry, community partners and the public.

Government funding underpins Netsafe's statutory and contracted services, and much of Netsafe's scams support, prevention, public education, research and innovation relies on short-term grants, corporate partnerships, philanthropy and donations.

A diversified funding base helps Netsafe maintain its independence, respond to emerging harms and ensure people are not left without support.

Much of Netsafe's funding is time-bound or project-specific. No funder directs Netsafe's casework, policy positions or public advice. This independence allows Netsafe to advocate for the safety of New Zealanders without compromising its independent judgement.

Industry investment also reflects shared responsibility. Organisations that benefit from the digital ecosystem have an important role in reducing its risks and supporting independent harm-prevention initiatives for the public good.

Case for support – the investment online safety requires

Netsafe maintained timely services despite record demand, but sustained performance should not be mistaken for unlimited capacity.

When funding does not keep pace with demand, inflation, complexity and expectations e.g. AI safety, digital literacy and wearable tech safety, the eventual choices are unavoidable: people wait longer, fewer harms can be prevented and services may be narrowed.

Demand for Netsafe's statutory HDCA service increased by 22% this year. However, the underlying funding settings remain anchored to 2021 cost assumptions and have not kept pace with cumulative cost increases, growing case complexity or demand.

At the same time, the services that identify emerging harms, prevent escalation and support people outside government-funded pathways remain the most dependent on charitable funding.

Diversified, multi-year investment helps prevent the consequences of constrained funding from falling on New Zealanders seeking help. It protects the frontline response people rely on while extending prevention, research and practical tools to communities before harm reaches crisis point.

Netsafe is seeking funding partners who want to prevent online harm earlier, reach underserved communities and build practical responses to online and AI-enabled abuse, scams and exploitation.



REVENUE MIX BREAKDOWN

Funding source	Percentage
Community	3%
Corporate	2%
Government	86%
Industry & tech sector	3%
Philanthropy	6%

Statement of Revenue & Expenditure

	FY26	FY25
REVENUE		
Revenue from exchange transactions	**$6,549,635**	$6,064,469
Revenue from non-exchange transactions	**$819,605**	$824,294
Total revenue	**$7,369,240**	$6,888,763
EXPENSES		
Administration expenses	**$310,723**	$314,652
Audit fees and consulting fees	**$360,354**	$305,879
Other operating expenses	**$1,986,653**	$1,836,997
Staff expenses	**$302,347**	$471,993
Wages and salaries	**$4,502,009**	$4,408,898
Total expenses	**$7,462,086**	$7,338,419
FINANCE INCOME		
Interest, dividends and other investment revenue	**$2,253**	$29,595
Total finance income	**$2,253**	$29,595
Net surplus/(deficit) for the year	**-$90,593**	-$420,061
Total comprehensive revenue and expenses for the year	**-$90,593**	-$420,061

Statement of Financial Position

	FY26	FY25
CURRENT ASSETS		
Cash and cash equivalents	**$1,225,961**	$951,714
Prepayments	**$153,308**	$164,999
Receivables from exchange transactions	**$1,236,637**	$1,613,371
Receivables from non-exchange transactions	**$203,000**	-
Total current assets	**$2,818,906**	$2,730,084
NON-CURRENT ASSETS		
Property, plant and equipment	**$122,527**	$139,226
Intangibles	**$612,999**	$642,143
Other non-current assets	**$68,956**	$499,210
Total non-current assets	**$804,482**	$1,280,579
Total Assets	**$3,623,388**	$4,010,663
CURRENT LIABILITIES		
Payables from exchange transactions	**$138,990**	$362,117
Employee benefits	**$580,662**	$521,905
Goods and services tax	**$82,633**	$83,534
Income in advance	**$70,725**	$202,137
Total current liabilities	**$873,010**	$1,169,693
Total liabilities	**$873,010**	$1,169,693
Total net assets	**$2,750,377**	$2,840,970
EQUITY		
Accumulated surpluses	**$2,750,377**	$2,840,970
Total equity	**$2,750,377**	$2,840,970

netsafe

Appendix 1: Data sources

This appendix provides supporting information for the Year in Review, including the sources and notes underpinning reported data.

Platform audience estimates

These notes relate to the “Reports by Platform: New Zealand” infographic in the section “Where online harm is being reported in New Zealand”.

The platform audience figures combine advertising-reach estimates from DataReportal and app-activity estimates from Sensor Tower. They are indicative audience sizes, not directly comparable monthly active-user figures. The “share of combined top-10 audience” represents the share within the ten platforms included in the report only; users overlap substantially across platforms.

- TikTok covers the advertising audience aged 18 and over only; YouTube, Facebook and other DataReportal estimates include people aged 13 and over.
- WeChat’s estimate of 180,000 has been carried over from the previous report and remains unverified because no reliable recent public New Zealand source is available.
- The difference between audience share and report share is descriptive only and should not be interpreted as statistical under- or over-representation.

Platform	Latest NZ audience estimate	Share of combined top-10 audience	Report % share (FY26)	Diff (report – audience, pp)	% HDC (FY26)
YouTube	4,240,000*	23.9%	2.6%	−21.3	70%
Facebook	3,450,000*	19.4%	32.5%	+13.1	78%
Instagram	2,650,000	14.9%	19.3%	+4.4	86%
TikTok	2,040,000*	11.5%	23.0%	+11.5	83%
WhatsApp	2,760,000	15.5%	6.7%	−8.8	73%
Snapchat	1,460,000	8.2%	9.0%	+0.8	87%
X/Twitter	678,000	3.8%	2.3%	−1.5	67%
Discord	278,000	1.6%	3.0%	+1.4	87%
WeChat	180,000†	1.0%	0.9%	−0.1	88%
Tinder	37,300	0.2%	0.6%	+0.4	71%

Sources

YouTube, Facebook, Instagram, TikTok, Snapchat and X/Twitter:

DataReportal, Digital 2026: New Zealand, published 8 November 2025. https://datareportal.com/reports/digital-2026-new-zealand

WhatsApp and Discord:

Sensor Tower, Top 5 Communication Apps Performance in New Zealand, Q4 2025. https://sensortower.com/blog/2025-q4-unified-top-5-communication-apps-units-nz-6070aae1241bc16eb81f5bab

Tinder:

Sensor Tower, Top 5 Dating Apps in New Zealand, Q4 2025. https://sensortower.com/blog/2025-q4-unified-top-5-dating-units-nz-64c9b6bbe1714cfff1c9d0e8

WeChat:

No reliable recent public New Zealand estimate is available. The figure of 180,000 is carried over from the previous report, which cited the World Population Review country table labelled "WeChat Users 2021", and should be treated as unverified. https://worldpopulationreview.com/country-rankings/wechat-users-by-country

Population:

5,342,000 — Stats NZ, National population estimates: at 31 December 2025. https://www.stats.govt.nz/information-releases/national-population-estimates-at-31-december-2025/

Appendix 2: Case Studies

The case studies illustrate the types of online harm, support and outcomes discussed throughout this report. They are based on real experiences of people supported by Netsafe. Names and identifying details have been changed or omitted to protect privacy. They illustrate individual experiences and should not be interpreted as representative of everyone who contacts Netsafe.

1: Deepfake videos used to target a young person

When Olivia (not her real name), a student at a large secondary school, discovered a deepfake video of herself on TikTok, the impact was immediate.

The anonymous account had been created specifically to target students and staff from her school, sharing multiple AI-generated videos designed to embarrass, humiliate, harass and bully those depicted.

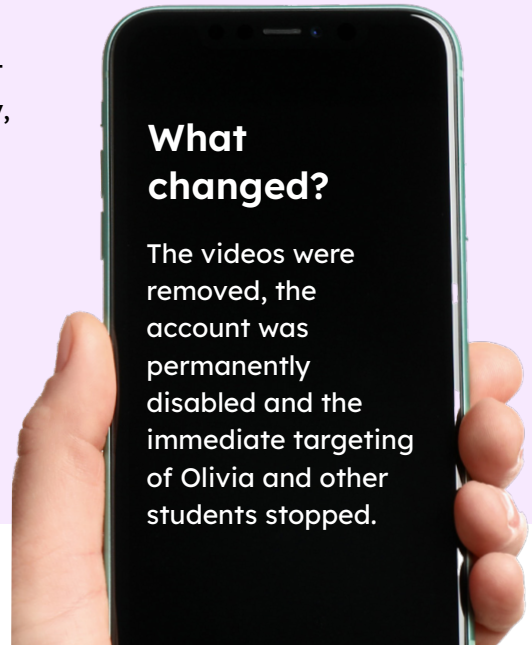
Although the video was fake, the harm was real. Olivia felt overwhelmed and anxious. She worried about how classmates would react, whether people would believe the content was genuine, and whether more videos would appear. Feeling frightened and unsure what to do, she reached out to Netsafe for support and advice.

Netsafe explained that AI-generated content used to humiliate, harass or bully someone can have a serious impact, even when it is obviously fake. Olivia was encouraged not to engage with the anonymous account, to take screenshots and record the account details, and to seek support from trusted adults and her school. Netsafe also outlined the reporting options available under the Harmful Digital Communications Act and reinforced the importance of looking after her wellbeing while the matter was being addressed.

Netsafe contacted TikTok to report the content and account. TikTok removed the videos and permanently disabled the anonymous account, stopping the immediate targeting and reducing the risk of further harm to Olivia and others at the school.

This case shows how generative AI is creating new online safety challenges. Deepfakes do not need to be explicit or realistic to cause harm: embarrassing or humiliating AI-generated content can affect a young person's confidence, sense of safety and willingness to participate in school life.

It also demonstrates the value of timely support that helps people respond safely, preserve evidence and access the right reporting pathways.



2: An emerging form of online dependency — AI companions

"Louise" (not her real name) contacted Netsafe with a question many people may increasingly ask: "Should I be worried that I talk to AI so much?" She had started using AI as a regular source of conversation and comfort but became concerned about the personal details she might be sharing.

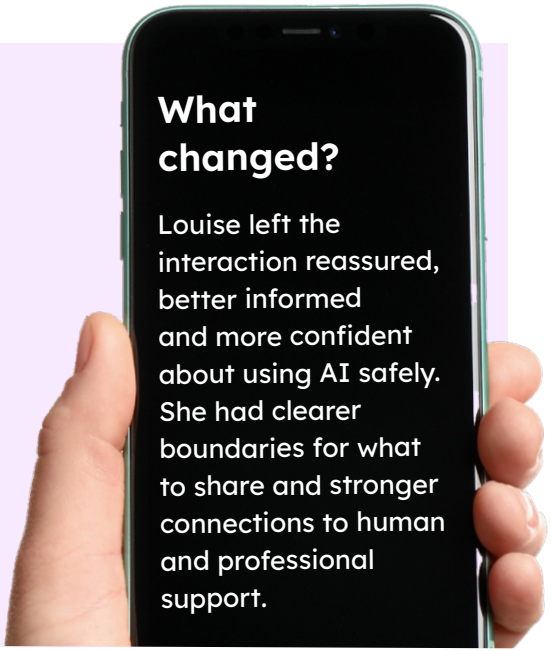
Her question highlights an emerging online safety issue. As AI becomes easier to access and more human-like in conversation, people may turn to it for comfort, reflection and companionship without fully understanding how their information is used, stored or personalised.

Louise said AI had become more than a tool: "It feels like the friend I used to have." She knew it was not a real person, but it was always available to listen. Counselling had helped in the past, but when support was not available, she increasingly turned to AI when she wanted someone to talk to.

One conversation unsettled her when the AI used her first name, although she could not remember providing it. Netsafe explained that some AI tools can personalise conversations using information linked to a user's account or login, not just details typed into a single chat.

Netsafe reassured Louise that she was not alone in having questions about AI companionship. The team explained that AI can provide a useful space to organise thoughts, practice conversations or reflect, but it is not a substitute for genuine human relationships or professional mental health support.

Netsafe encouraged Louise to keep speaking with her GP and health coach, and to seek counselling or mental health support when isolation felt difficult. Netsafe also reminded her to avoid sharing sensitive information, such as financial details, identity documents, passwords or her home address, and to treat AI responses cautiously because they can be inaccurate or misleading.



3: When intimate images become a tool of coercive control

When Nicole (not her real name) ended a five-year relationship, she hoped the abuse would stop. Instead, it escalated.

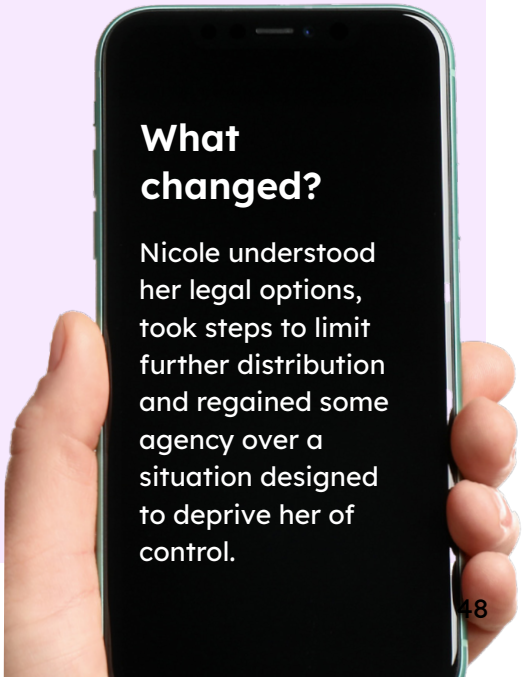
Over several years, her former partner had pressured her into sending intimate images. After the relationship ended, he shared those images with strangers online and used AI tools to create fake sexually explicit videos depicting Nicole, distributing them through multiple messaging platforms. He also threatened to create an OnlyFans account using her images, continued contacting and stalking her despite a protection order, and threatened suicide.

For Nicole, the harm went far beyond the internet. She felt afraid, violated and unsafe, not knowing who had seen the images or where they might appear. The ongoing threats affected her sleep, appetite and physical health, leaving her exhausted and emotionally drained.

When Nicole contacted Netsafe, the team helped her understand her options and how to take practical steps to reduce further harm. Netsafe explained that sharing, or threatening to share, intimate images without consent may be covered by New Zealand's Harmful Digital Communications Act, including AI-generated intimate deepfakes. Netsafe also explained that consent given within a relationship does not mean consent for images to be shared later, and that consent can be withdrawn.

Netsafe helped Nicole preserve evidence, report harmful content and accounts, use tools such as StopNCII.org to remove images from the internet, and understand how platforms could be approached to seek removal without her having to provide copies of the intimate images. Netsafe supported Nicole with the digital harm aspects of her situation, while she also received help from Police and Women's Refuge.

This case shows how intimate image abuse and AI-generated sexual deepfakes can be used as tools of coercive control, affecting safety, wellbeing, autonomy and recovery after abuse.



4: Takeshi's story: When a legitimate-looking translation job became a scam

Takeshi's (not his real name) experience shows how sophisticated employment scams can exploit legitimate-looking freelance work, and how early advice can help reduce the risk of further financial and identity harm.

Takeshi was an experienced translator when he accepted two translation jobs worth USD $3,800 and USD $4,000. The rates seemed reasonable, contracts were signed, and his completed work was accepted and praised as "excellent".

When it was time to be paid, Takeshi was told the funds had been transferred to an account with "Wealth Evolution Bank". The money appeared to be available online, but when he tried to withdraw it, he was told he first needed to pay USD $700 for a US VAT number—a fee he was assured would later be refunded.

The request escalated quickly. Takeshi was directed to a cryptocurrency website, then asked for his card CVV and PIN when his payment failed. He refused to share them. He was then instructed to transfer the USD $700 to a Japanese bank account, but because the final confirmation step was missed, the payment did not go through.

Takeshi had already shared copies of his passport and driver licence, along with his address and phone number. He was worried about identity theft, misuse of his financial information, and the translation fees he had never received. The documents he shared could potentially be used to impersonate him, access accounts or set up fraudulent services in his name.

Netsafe helped Takeshi recognise the scam, preserve evidence and prevent further harm by ending contact, stopping payments, alerting his bank and recommending to him that he replace compromised identity documents and passwords.

Employment and task scams can look highly convincing. They may involve signed contracts, professional communication, completed work and fake online platforms showing money supposedly waiting to be withdrawn. A major warning sign is being asked to pay money to receive money, particularly through cryptocurrency or other difficult-to-recover methods. Requests for passwords, PINs, card details or identity documents should also be treated with caution.

Netsafe's Get Set Up for Safety hub at netsafe.org.nz, includes guides for spotting and responding to scams, while CheckNetsafe, a free tool that helps people check whether a website or link may be safe before clicking on it, can help people check suspicious websites and links.

