28 November 2023

Hon Brooke van Velden
Minister of Internal Affairs
brooke.vanvelden@parliament.govt.nz

Tēnā koe e te rangatira

Netsafe briefing to incoming Minister of Internal Affairs - online harm in Aotearoa New Zealand

Congratulations on your election and appointment to the Internal Affairs portfolio. You're likely to be scanning briefings from officials to inform your thinking on priorities. As you do, please consider our briefing on online harm alongside briefings from your department.

The attached briefing tells you about Netsafe, the work we do with government and community, and rising levels of online harm in Aotearoa New Zealand. In this letter we focus on Netsafe's role in the online safety eco-system and the areas where we think you can make a difference. We also set out priorities in the justice and education spaces because of a previous decision by the outgoing Labour Government which proposed that the Department for Internal Affairs should have responsibility for the administration of the Netsafe contracts from the Ministry of Justice and the Ministry of Education from 1 July 2024 (see more on this below).

Netsafe and the online safety eco-system
Netsafe is New Zealand's independent online safety organisation with a 25-year history. We:

- are an incorporated society and a charity with online safety at our core and we are also the appointed Approved Agency under the Harmful Digital Communications Act 2015
- are a member and Vice President of INHOPE (until 2025), the global network of 52 member hotlines, leading the fight against CSAM online. Inhope is adjacent to government and law enforcement but is a civil society response to the fight against CSAM and
- receive over [28000] reports every year from New Zealanders who have experienced the full range of online harms.

Online safety and digital safety are distinct from *cyber security*. Cyber security is a subset of national security policy. Cyber security concerns protecting people and their computers, networks, programs, and data from unauthorised access, disruption, exploitation or modification.

We partner with the community to run campaigns and programmes to support groups of New Zealanders being targeted online. This currently includes a national sextortion campaign, the Women's Online Safety Partnership, Youth Ambassador in Schools Programme and a partnership with Chorus to support seniors with scam education. Support and resources are also provided to schools and kura.

Netsafe is part of a broader eco-system that includes online safety, digital safety and cyber security. Netsafe's focus is primarily on *online safety - the people and behavioural side of digital and online spaces*. We also work with the Police, Classification Office, Customs, and the Department of Internal Affairs on *digital safety.* For example, Netsafe refers child sexual abuse material (CSAM) and violent extremist content to the DIA Digital Safety Team.

While there are distinctions between online safety and cyber security, the two are linked. Safety starts outside the device and in particular it is important that youth and seniors develop skills around media and online literacy and good digital citizenship. We therefore work with the Cyber Emergency Response Team (CERT) and Network for Learning to support online security in the community and schools.

Netsafe's funding contracts with the Ministry of Justice and Ministry of Education (and decision of former government to transfer administration of the contracts to DIA)

As you may know Netsafe is currently funded by MOJ to carry out our Approved Agency functions under the HDCA (until 2026) and MOE to provide support and resources to schools and kura (until 30 June 2024).

At the end of the last parliamentary term, the previous Government decided to transfer Netsafe's contracts with MoJ and MoE to DIA and for this to take effect in July 2024.

We understand this came about because of work to align cybersecurity across government. However as neither Netsafe MOJ or MOE were consulted, the consequences and effects of this transfer have not been properly analysed or considered.

We do not think this decision makes sense given DIA is not otherwise the Government Department responsible for justice or education functions. We therefore ask that the new Government reverse the decision.

Apart from taking on functions for which it is ill suited, we do not think DIA should control both the agenda and core funding for online safety. While DIA has grouped its censorship, spam and objectionable content functions under the heading digital safety, it does not have experience with the portfolio specific online safety work we do. More importantly, there is a distance and independence between Netsafe and Government involvement in the censorship and objectionable and regulatory environment that needs to be maintained.

In the event that the new Coalition Government decides to push ahead with this contract transfer, as well as matters that you ought ordinarily to be aware of as DIA minister, then we also include in this briefing the justice and education functions. At **Attachment A** we have captured the justice issues affecting the online safety space for your consideration. At **Attachment B** we have captured the education functions for your consideration.

Policy work on safer online services and media platforms

As you will know, the last Government undertook policy work on safer online services and media platforms and the DIA consulted on proposal in July last year. Netsafe's responded to that consultation and our response can be found here. One of the main comments we made was that we did not think this work sufficiently considered the role the HDCA plays in dealing with harmful online content. If the DIA work on safer online services continues, we recommend that it consider the HDCA in more detail. We think that an updated HDCA could address several of the issues raised in the consultation without the proposed centralisation of online safety services.

Netsafe is well placed to deliver online safety services in a public private/NGO partnership

After 25 years providing online safety education and support, Netsafe has become a well-known and trusted brand. More than 60 percent of New Zealanders describe themselves as aware of Netsafe. As an NGO we are able to tap into partnership opportunities that are not available to government (such as membership of the Meta Safety Advisory Board, and our trusted flagger relationships).

The previous Government ran a two-year digital safety campaign called Keep it Real Online. In 2022 the campaign got a dedicated website keepitrealonline.govt.nz and opened a direct to student channel using third party vendors to deliver online safety content to students, parents and youth. However, no endorsements for demonstrating that the third party programmes are evidence-based and curriculum aligned is apparent from the published online materials.

> Should you be thinking about whether online safety education services may be better delivered externally under contract to the DIA then Netsafe and the Ministry of Education (MOE) have spent some time developing a trusted service provider programme to make sure that the curriculum and content being taught by third parties related to online safety is fit for purpose. The trusted service provider program, combined with the Keep it Real portal, could take the guesswork out of identifying a great online safety education provider for communities. Netsafe is well placed to manage the Keep it Real programme under contract, and improve its content and reach, and give it the 'backed by Netsafe' endorsement to appeal to parents and youth.

A meeting to discuss

Netsafe would very much appreciate a meeting with you to introduce ourselves and discuss online harm and education. Barb Wright, our Executive Assistant can be contacted at barbw@netsafe.org.nz and by phone on +64 21 925 910 and she can make meeting arrangements.

Congratulations again and I look forward to working with you and the incoming Government.

Ngā manaakitanga

Brent Carey
Chief Executive Officer

Appendix A: Key issues arising from the Justice portfolio

The key online harm issues for the Justice aspects of the portfolio are the need to update and strengthen the HDCA, increasing harm reports, support for victims of online crimes and enhancing alternative dispute resolution practices, social media and youth offending, victim support, and stalking and harassment. We discuss each below.

Stalking and harassment

We are seeing a dramatic increase in the amount of stalking and harassment online, which can lead to physical and sexual violence. At the moment harassment is covered in a piecemeal way, across different pieces of legislation, including the Harassment Act, the Family Violence Act and the HDCA. Since 2020, successive Ministers of Justice have acknowledged the legislation needs to be reviewed, but work has stalled. We recommend you add stalking and harassment to your law reform programme.

Victim recovery

There is a gap at the moment in victim recovery programmes for people who experience online harm. Survivors of online harm (many of whom are repeat victims) are asking Netsafe to do more to support them recover from online harm.

If Netsafe was funded to place greater focus on victim remediation Netsafe would like to partner with the likes of the Victims Support agency and other victim-centric Justice sector agencies to develop guides (in various languages) that are not victim blaming, and help victims understand their rights and get access to recovery materials and support so they can rebuild their lives.

Justice responses to image-based sexual abuse often fall short of expectations

We need trauma-informed approaches to policies and practices across all sectors responding to image based sexual abuse. Better training and education of law enforcement is needed.

The HDCA needs to be revisited again to consider whether the Act could be more victim-centric when it comes to image based abuse.

Finally consideration should be given to inclusion in law of an expansive definition of what constitutes an "intimate image" in line with different cultural norms and standards.

The Harmful Digital Communications Act urgently needs an update

The HDCA has a number of limitations and is in need of updates. The limitations include its focus on individuals, not groups as targets of online harm. There have also been advances in technology being used to cause online harm. For example, the HDCA does not explicitly prohibit abuse using artificial intelligence (AI), which is becoming increasingly common. AI allows the creation of deep fake or synthetic intimate images depicting real people in situations that are not real. These can then be shared online and used for threats or blackmail.

Netsafe recommends a review of the HDCA and has attached a high level summary of some potential topics that could be considered as part of the scoping for any review.

The previous Government's Safer Online Services, Media and Platforms discussion paper does not seek to reform any laws where content is already objectionable and harmful, or provide more support for victims. This necessitates strengthening the HDCA and existing structures dealing with illegal content and activities. This would be a better course compared to the untested Safer Online Services, Media and Platforms change agenda.

Harm reports to Netsafe are at record numbers. Complaint forecasts to the end of the financial year 30 June 2024 have us on track to record more than 7000 HDCA complaints. This will see us exceed our 3.9 million appropriation by approximately $200,000. We have signalled this to the Ministry at the end of quarter 1 and sought assurance that the Ministry of Justice will seek funds from its broader appropriation in which the Netsafe contract sits to pay for peak complaint demand.

Netsafe suggestions for issues to consider as part of a review of the HDCA

The following suggestions for issues to consider as part of a review of the HDCA have been discussed with the Ministry of Justice.

General improvements

- Most phone calls are technically digital communications as defined in the HDCA. Clarity is needed on whether these should be caught by the legislation.
- Potential loopholes:
    - Airdrop, encrypted data, live stream, and disappearing messages are considered digital communications even though they are fleeting and the digital evidence no longer exists or is not readily accessible
    - Data that is being shared or has been shared by a private account, that can only be accessed by the account holder or friends
    - A threat to share (communicated digitally) is treated the same as content that has been shared.

Individuals and groups

There are a number of areas where the Act's focus on individuals is a problem:

- Harmful speech targeted towards groups is a potential gap in the legislation because it may not identify any one or particular individual. Consideration of whether the Act should include redress for members of a group who have suffered harm more generally but where an individual is not specifically targeted is needed.
- Small businesses where the content is damaging to a specific individual (e.g. sole trader) and they suffer harm.
- School leaders cannot consent to engage in the dispute resolution process on behalf of a student. But they can do so in their own right.

Other

- There is nothing explicitly requiring a connection/ nexus to New Zealand in the legislation which raises jurisdiction and demand for services issues. People in New Zealand as tourists or the wider Pasifika diaspora asking Netsafe for help from overseas. Dealing with people who are overseas is challenging from an evidentiary and service level position.
- There is no Privacy Act carve out for dealing with harmful digital communication matters (section 29).
- Make it clear that the existing prohibition on posting intimate visual recordings without consent clearly covers synthetic or deep fake images where a victim could be identified.
- There are repeat reporters (victims of online harm) who report issues to Netsafe but don't engage with the courts processes beyond Netsafe. We keep issuing case summaries, but they refuse to go to the District Court for remedies. Should there therefore be discretion to not have to produce a case summary unless it is necessary for a Court proceeding?
- Police taking civil cases. To our knowledge, the Police have never taken a civil case against an individual under the HDCA and therefore are not using all the enforcement provisions of the HDCA.

- Mis/dis/malformation is plentiful but is rarely a breach of the communication principles in the HDCA.
- False allegations is typically in the top three comms principles breached. For example, accusations of rape, paedophilia, drug use, infidelity, fraud. Netsafe has no powers to investigate. It is not typically a breach of platform community standards without evidence; so can't usually offer any redress except via the district court processes.
- Consider the use of restorative justice solutions and other more victim centric processes. Also consider making the Youth Court (not the District Court) an option for people under 18 years old wanting to resolve their HDCA matters.
- Consider prescribing (under section 7(b)) additional functions such as tackling harms related to body dysmorphia and eating disorders, adult content in video games and cyberflashing.

Appendix B Key issues from the Education portfolio

Netsafe work in schools and with young people and their families in a public/private partnership model
Netsafe provides support and resources for schools, kura and parents dealing with young people and online harm. This includes:

- An online learning management system (and content) for schools and kura, presentations by Netsafe staff, and classroom resources.
- Resources on our website for parents and youth, for helping young people with online bullying, safe online relationships, security, and 'sexting'.
- Support and advice to schools and kura from Netsafe when dealing with online incidents.
- Calls by parents and teachers to our seven day a week helpline.
- The Youth Action Squad, a programme that supports students to enact positive changes around the online safety issues that affect them most.

We regularly ask schools and kura to evaluate the services we provide, through a satisfaction survey. Ninety-three percent of respondents, from the last quarter, rated their experience of our face to face and webinar services as 8/10 or higher.

Young people are particularly vulnerable to cyberbullying and online abuse. We are seeing a dramatic increase in sextortion, and a number of issues made worse through online platforms, such as youth suicide, body image issues, posting and boasting about criminal activities, and the spread of misinformation and disinformation.

More services are required to educate and support young people and their digital lives. As Minister of Education you have two levers to do this: through the curriculum, and through Vote Education funding for programmes and resources.

Netsafe recommends that you:

- Update and improve online safety and (social) media literacy as part of the curriculum for schools and kura. We also suggest you re-examine the decision to remove media literacy from Curriculum Level One, because the age of criminality under the Harmful Digital Communications Act applies from the age of 10.
- Invest in anti-cyberbullying programmes in schools. For example, the localisation of Ireland's *Fuse* program to counter cyberbullying https://antibullyingcentre.ie/fuse and make Netsafe the New Zealand home of this global programme.
- Improve reporting pathways to Netsafe regarding online harm incidents in schools and kura.
- Fund more Netsafe bite sized micro-learning moments (less than 20 minutes each) to teach young people about responsible technology use. Six have already been launched successfully funded by the Ministry of Education (MOE) with three more under development to roll out in Term 1 in 2024.
- Fund research to address content that sexualises children or depicts self-harm and suicide violence against children.

We think the proposed ban on phone use during school term could complement the suggested update to the curriculum, to educate students about social media use, technology, and screen time.