



28 November 2023

Hon Melissa Lee
Minister for Media and Communications
melissa.lee@parliament.govt.nz

cc: matthew.stephens@parliament.govt.nz

Tēnā koe e te rangatira

Netsafe briefing to incoming Minister for Media & Communications - online harm in Aotearoa

Congratulations on your election and appointment to the Communications 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 in Aotearoa, alongside briefings from your department.

While issues concerning online harm have not traditionally been the responsibility of the Minister of Communications, they are part of the broader eco-system of which your portfolio is a part. Government investment in high quality connectivity means that New Zealanders have the internet access they need to participate in the online world. This brings many economic and social benefits. The online world can also be complex and harmful at times.

The attached briefing to incoming ministers 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 highlight a number of issues we have raised with the ministers responsible for the Internal Affairs, Education and Justice portfolios. Making progress in each of these areas will require cross-portfolio support. We hope you can support Netsafe to get the traction that is needed.

Netsafe is part of an eco-system that deals with online harm, cyber safety and security

Netsafe is part of a broader eco-system that includes online safety, cyber safety and cyber security. Our focus is primarily on *online safety* - the people and behavioural side of the online world. Online safety services include incident management, counselling, education, victim remediation and helping people to navigate social media responsibly. We also partner with the community to run campaigns and programmes to support groups of New Zealanders being targeted online.

The *digital safety* part of the eco-system includes dealing with child sexual abuse material (CSAM), violent extremist content and unsolicited commercial electronic messages (spam). Digital safety is handled by the Digital Safety Team at the Department of Internal Affairs (DIA), Police, and Classification Office. Netsafe has a role referring CSAM and other objectionable content to the agencies with enforcement and other functions in this area. It also has trusted flagger relationships with the online platforms most commonly used in New Zealand, which provide rapid escalation options to get harmful content removed.

Online safety and digital safety are distinct from *cyber security*. Cyber security is a subset of national security policy. Cyber security means protecting people and their computers, networks, programs, and data from unauthorised access, disruption, exploitation or modification. Government agencies working in this area currently include Cyber Emergency Response Team (CERT), the National Cyber Security Centre (NCSC), and the National Cyber Policy Office (NCPO). Cyber security has in the past been part of the National Security and Intelligence Portfolio and delegated to the Communications Minister.

There are of course overlaps between the three parts of the eco-system, and online safety and cyber security 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. Netsafe therefore works with the Cyber Emergency Response Team (CERT) and Network for Learning to support online security in the community and schools.

Online harm and education

Netsafe provides support and resources for schools, kura and parents dealing with young people and online harm. From our work we know that 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. We have asked the Minister of Education to help make this happen, by making changes to the curriculum for schools and kura, and through Vote Education funding for programmes and resources.

On the curriculum side, we need to update and improve the focus on online safety and social media literacy. There is very little in the existing curriculum that prepares young people to adequately engage (and stay safe) in a complex online world. We think the proposed ban on phone use during school term (in the National manifesto) could complement the suggested update to the curriculum, to educate students about social media use, technology, and screen time. This issue also has some urgency because the age of criminality under the Harmful Digital Communications Act applies from the age of 10.

On the programme and resources side, the Government needs to invest in anti-cyberbullying programmes in schools and kura, support the development of new resources for teachers (including Netsafe's micro-learning moments), and fund research to address content that sexualises children or depicts self-harm and suicide violence against children.

The Harmful Digital Communications Act (and the Justice portfolio)

Netsafe is the approved agency under the Harmful Digital Communications Act 2015 (HDCA). The HDCA was passed by the last National Government, to address online bullying, harassment, abuse and intimidation. We provide a seven-day-a week helpline, community presentations, resources for the victims of harm online, proactive advice on how to stay safe online, and an alternative dispute resolution service to resolve complaints between individuals and with the internet industry (e.g. platforms).

We have advised the Minister of Justice that the HDCA is urgently in need of an update to address new forms of online harm. The limitations of the existing legislation 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 is of the view that updating the HDCA would be a better course compared to the proposals from the previous Government as part of its Safer Online Services, Media and Platforms change agenda. Those proposals did 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.

We have also briefed the Minister of Justice on:

- concerns about the contribution of social media to youth offending (an issue that has to date fallen between the cracks of agency responsibility)
- the need to educate youth about the implications of social media being an aggravating factor at sentencing
- the dramatic increase in the amount of stalking and harassment online (harassment is currently covered in a piecemeal way across different pieces of legislation)
- gaps in victim recovery programmes for people who experience online harm
- the need for better training for law enforcement personnel, to be able to deal with image based sexual abuse.

Netsafe funding contracts

Netsafe is currently funded by the Ministry of Justice (to carry out functions under the HDCA, until 2026) and the Ministry of Education (to provide support and resources to schools and kura, until 30 June 2024). Our relationships with these agencies are critical to meeting education needs, and ensuring we can effectively play our part in the broader justice system that the HDCA is a part of.

At the end of the last parliamentary term, the previous Government made a rash decision to transfer Netsafe's funding contracts to DIA and for this to take effect in July 2024. We understand this decision was collateral damage resulting from a broader piece of work to align cybersecurity work across government, and a throwaway comment related to cyber safety, without any benefits analysis or consultation with the Ministry of Justice, Ministry of Education or Netsafe.

We ask that the new Government reverse the decision, so that Netsafe continues to contract with the Ministries of Justice and Education. DIA should not 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.

We are seeking your support to have the decision of the previous Government reversed.

A meeting to discuss

Netsafe would very much appreciate a meeting with you to introduce ourselves and discuss online harm in Aotearoa New Zealand. 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