Draft Aotearoa New Zealand Code of Practice for Online Safety and Harms: Public Feedback

Organisation responding: The Internet Watch Foundation (IWF)

Address: Internet Watch Foundation, Discovery House, Chivers Way, Vision Park, Histon, Cambridge, United Kingdom, CB24 9ZR

Contact details of the person responding: Abigail Fedorovsky, Policy and Public Affairs Officer, abigail@iwf.org.uk

1. About the Internet Watch Foundation (IWF)

1.1.The Internet Watch Foundation (IWF) is an international hotline based in the UK which provides a secure and anonymous place for over 2.5 billion people globally to report suspected child sexual abuse material (CSAM) in their local language. If these reports are confirmed as CSAM, our analysts work to have that imagery removed from the internet, wherever it may be hosted in the world.

1.2.The IWF's vision is an internet free from child sexual abuse and we are a charity that works in partnership with the technology industry, law enforcement (including Interpol), and other Governments globally to achieve that aim.

1.3.The technical tools and services we provides help to keep technology companies' platforms and services free from CSAM. The IWF has over 170 members from the internet industry who deploy our services to combat the spread of CSAM on their platforms.

1.4.**In 2021 we assessed and removed 252,000 webpages confirmed as containing CSAM from the internet. Each of these can contain from one to thousands of individual images or videos, so this is millions removed last year.**

1.5.Along with 45 other hotlines around the world, the IWF is part of the International Association of Internet Hotlines (INHOPE.)

1.6.**In 2020, more than half (57%) of all the unique child sexual abuse URLs exchanged through INHOPE's database were identified by the IWF.**[1]

[1] This data is not yet available for 2021.

1.7. We are also one third of the UK Safer Internet Centre, a partnership of three organisations working to make the internet a safer place for children through providing our hotline, helplines and an awareness centre with educational resources for children, their parents, and schools.

2. Summary

2.1. We would like to thank NetSafe for the opportunity to provide feedback on this draft voluntary code. We appreciate the work that has already gone into consulting with platforms to develop the document, and welcome the ongoing collaboration to ensure this is as effective as possible.

2.2. As the UK's hotline for assessing and removing CSAM for over 25 years, we believe we can contribute unique insights that might help New Zealand when it comes to tackling illegal content online.

2.3. We welcome many aspects of the draft code, including the focus on a systems-based approach to best practice standards, the emphasis on collaboration and cooperation (including across borders) and the ambition that users will be more empowered to make informed decisions about the content they see. We particularly welcome Outcome 1 and the priority focus on platforms "[providing] safeguards to reduce the risk of harm arising from online child sexual exploitation and abuse."

2.4. That being said, we have a few recommendations to offer from our own work:

- **Providers should be expected to sign up for hash and blocking lists from hotlines and law enforcement agencies.**

- **The Administrator should collaborate with hotlines around the world to inform assessments about the quantity of illegal content on platforms.**

- **The Administrator should ensure that they are aware of new and emerging trends, and should then liaise with platforms about how best to tackle these.**

- **Providers should ensure that they are able to keep their platforms free from CSAM, even within encrypted channels.**

3. Adopting hashing technology.

3.1. Many hotlines and law enforcement agencies around the world have created hash lists and blocking lists, for instance the IWF's hash list currently has one million unique images on it. We are working with the UK Government to add another two million by 2023.

3.2. We know that the majority of CSAM on the internet is duplicates of the same or video, for instance US law enforcement confirmed to one victim that they knew of over 70,000 instances where her image had been shared. Platforms can use hash lists both to scan and remove duplicates, but also to prevent the duplicates being reuploaded at all.

3.3. We also know that blocking lists can be highly effective. In just one month in 2020, three of the IWF's member companies counted 8.8 million attempted hits to our blocking list by UK users alone. This is 8.8 million times that users were unable to access known illegal content.

3.4. We believe that this voluntary code should strongly urge platforms to sign up to both these types of lists, to ensure that users are not knowingly or accidentally accessing CSAM.

3.5. It is also important that the Administrator collaborates with hotlines who have expertise in assessing and removing illegal material, to better understand where the content is being found and ensure that platforms act when there is a problem.

4. New and emerging trends.

4.1. Given our role at the forefront of tackling CSAM, we often identify new trends and threats at an early stage. For instance, over the last two years, we have seen a particular rise in the number of "self-generated" or "first-person produced" indecent images online. This might include instances where a young girl is alone in her room and groomed into sexual activity in front of a webcam which is then captured and shared by the offender.

4.2. From January to September 2021, two out of every three reports our analysts assessed included this type of material (27% higher than 2020.)

4.3. Most of the victims that we see in this type of material are 11-13-year-old girls, however we are seeing a rapidly increasing number of 7-10-year-olds too. We believe it is essential that the Administrator is able to identify new trends such as these, and then liaise with platforms about the best ways to tackle this.

5. Encryption.

5.1. We think that it is important for this voluntary code of practice to mention end-to-end encryption, given the impact that we anticipate this having over the coming years. Many companies are moving to encrypt aspects of their platform, to increase privacy for users.

5.2. We strongly believe that privacy is important and that encryption is not bad in and of itself, however it is essential that companies should not be encrypting their services until they can ensure that appropriate child safety measures are in place.

5.3. We previously saw the impact in the EU when Facebook decided to stop scanning their platforms for CSAM because of the delays to the temporary derogation from the e-privacy directive. This led to a 48% reduction in CSAM referrals from EU accounts to the National Center for Missing and Exploited Children from December 2020.

5.4. It is essential that illegal material continues to be identified by the industry, and that the privacy of children is given upmost priority. Along with including encryption as a risk design choice within the voluntary codes, the Administrator could also specifically work with platforms to incentivise them to develop innovative solutions to continue scanning for illegal content in encrypted channels.

6. Conclusion

6.1. We welcome the introduction of a new code in New Zealand and believe that this is a step towards better online safety for children across the world. We look forward to continuing to work with NetSafe and coordinate with the Administrator as this takes shape.

6.2. We are pleased that the draft voluntary code focuses on the global nature of the internet and believe that it is essential for us all to work together from different nations to achieve an internet free from abuse and exploitation.