Social media safety and reporting harmful content guidelines

SS-GDL-003

Table of Contents

1. Purpose

The purpose of this guideline is to support and assist you as an individual in helping to keep yourself safe online. This guideline provides advice on social media security and how to respond to comments, harassment or other issues you may face online.

Scope

This guideline applies to all Kāinga Ora employees (including casual and fixed term employees), secondees and interns.

2. Introduction

Social media is a reality of modern life and the nature of our work means that we'll often be in the spotlight. Social media is also a fast changing environment, with new technology and trends developing all the time that we need to adapt to.

This makes it easy for people we work with to freely express their opinion and engage in robust discussions. We welcome feedback and the opportunity to improve our services. However, sometimes this content can become harmful to you or your family members and friends.

It's important that you talk with your People Leader if you're feeling upset or affected by work-related content on social media, such as:

- negative comments or conversations about you or the people you work with
- someone's privacy has been breached
- if you or someone you work with is being bullied, harassed, or directly targeted with comments that may cause harm.

Make sure you share your concerns as soon as possible with your People Leader and the Health, Safety and Security Team if you believe there is abuse that needs to be responded to.

Kāinga Ora has the Employee Assistance Programme you can also call on for assistance.

Policy and other supporting documents

See also:

- Digital Harm policy – operational policy relating to digital harm
- Kāinga Ora social media guidance – provides details about staff code of conduct when posting information online.

3. What are the options for responding to harmful content?

Talk to your People Leader

First of all, let your People Leader know this has happened and discuss options for support and how to respond. This may include internal reporting (see section 7 Escalating and Reporting digital harm internally) and external complaint processes through social media platforms or Netsafe (see next section below).

If you are aware of a post related to your role on a social media platform that has had an impact on your health, personal security or mental wellbeing, in addition to reporting this to you People Leader, also report it to:

- the Senior Security Advisor, and
- the Noggin 2 Incident Reporting System as soon as possible.

Further details is available in section 7 Escalating and Reporting digital harm internally.

Complain to Netsafe

All people in New Zealand are able to make a complaint to Netsafe about digital communications that are causing them harm, as outlined under the Harmful Digital Communications Act 2015.

This includes online/digital bullying, abuse and harassment, and when someone has put something online that:

- tries to get someone to hurt themselves
- shares intimate images without consent (shared nudes, sometimes called “revenge porn”)
- encourages other people to send harmful messages to someone
- most people would think is very offensive
- shares someone’s sensitive and/or confidential information without their permission
- makes a false allegation about someone
- puts someone down because of their colour, race, ethnic or national origins, gender, religion, sexual orientation, or disability
- is indecent or obscene
- threatens to hurt someone or damage their property
- relates to a fake online platform or application profile
- is causing harm to someone.

Community standards and policies

Social media platforms such as YouTube, Facebook, Twitter and Instagram have policies that outline what they deem is and isn't acceptable.

Social media platforms need to balance safety and freedom of speech. This means that they often allow content to remain even when some find it offensive. See section 6 of this guideline: How to report harmful content to social media platform.

Listed below are some guidelines available on the internet that you may find useful:

- YouTube community guidelines
- Instagram community guidelines
- Facebook community standards

We also follow the Te Kawa Mataaho Public Service Commission Social media guidance.

4. What you should do if you are targeted on social media because of your work

First steps

- Let your People Leader know and discuss any further support that may be required to keep yourself and others safe.
- Take accurate records, including a screenshot of the page and posts. Record the date and time the harmful content was published. Save any images or videos and record the full URL (web address) of the page.
- If the content breaches the policies and guidelines of the social media platform, report the content using the guidelines below.
- Log an incident using the Noggin 2 Incident Reporting System as soon as possible.

Protect yourself

- Do not retaliate or engage with the post or comments. Engaging can lead to an escalation and spread of abuse as other people or, in some cases, 'trolls' engage. (A troll is a person who starts or expands on arguments or deliberately upsets people on the internet by posting inflammatory, or off-topic messages in an online community.)
- Review, and if necessary, adjust your own privacy settings and consider what is visible to others. See Netsafe's site: How to use privacy settings on social networks.
- For your own wellbeing you may want to avoid reading the comments. Stop following the page or group where the harmful comments are being made or take a break from social media for a while.
- While you may want to see what is in the content, try to avoid watching it as increasing the view count can help spread the content further by boosting it in a social media site's algorithm.

- If a particular person is abusing or harassing you, or if you don't want to be visible to someone, consider blocking them.

If you are concerned about the immediate safety of yourself or others, call 111.

5. Keeping yourself safe online

Be vigilant with privacy settings

Each social media site has controls to help you protect your privacy. For example, the Facebook Help Centre allows you to see which sections of your profile you can edit. It also tells you how to secure your account so that you can prevent contacts, or other people, from tagging you without your consent.

Consider modifying your social media name

If you are concerned about being found on social media, consider using a pseudonym that differs from the name you use at work. This can enable you to still use social media with a lower risk of being discovered and harassed.

Pseudonyms could include going by:

- your unmarried/maiden name; or
- an older family name; or
- a full name if you socially have a nickname; or
- a nickname if you use your full name in work settings; or
- your first and middle name and no surname.

Note: You need to be aware that in some cases, choosing a pseudonym that is obviously not your own name or related to your name can violate the provider's terms of service. You could be locked out of your account as a result.

Do a web search on yourself

It's a good idea to do a web search for your name and other personal details online to see what is publicly available – you may be surprised by what you find.

Consider removing anything that could be used to identify you and any personal information.

Doxing

Doxing (sometimes spelt 'doxxing') is a type of online harassment where people share personal or identifying information about someone online without their consent. This could include a person's full legal name, address, place of work, phone number or contact details for family members.

In many cases people will dox a person using information they find available online. In other cases, people may access your private information through hacking into your account or guessing your password.

Netsafe has more guidance on the process to prevent or report issues on Doxing.

How to protect yourself from being doxed

Be cautious of what you share online: Usually, people looking to 'dox' a person will search for information that is listed online somewhere. Think carefully before sharing any personal details or information on a public profile or website as someone could try and use this information against you. You should be particularly careful when publically posting:

- pictures or posts that identify your house and address
- details of your plans (that is, where you or your family plan to go and when)
- pictures of your car that include the registration plate
- pictures or details of where you or your family work.

If you do want to share this information with a social media contact, consider using the private message function.

Use strong passwords: One of the ways people sometimes access personal information to dox someone is by guessing passwords to online accounts. Make sure you use a different password for each of your online accounts and ensure they are strong by following their advice: How to choose a good password. Also make sure you've got two-factor authentication set up on your online accounts for extra protection.

Report abuse before things get out of hand: In some cases, doxing can happen after people have had a disagreement online. Remember, someone doxing you is never okay. To keep yourself safe, it's sometimes best to use the 'report' and 'block' functionality to report abusive content rather than continuing an argument online.

6. How to report harmful content to social media platforms

Most harmful social media content needs to be self-reported. This means that the person being targeted will need to report the content themselves to the social media platform.

Not every post or comment will be removed when you report it. If you can specifically identify how it violates the platform's policies, privacy rules or New Zealand law there is a greater chance that action will be taken.

Reporting incidents on social media platforms

Most social media platforms will have links on their apps or website to 'report abuse/privacy violations'. These links can be used to report instances of abuse, defamation, privacy breaches or similar concerns.

Some examples of these links can be found below:

- Facebook's Defamation Reporting Form and Privacy Violation Reporting Form
- YouTube's Privacy Complaint Process
- Instagram's Report Violation Process

You can also report an incident directly to Netsafe:

- Netsafe's Report an Incident Page

Contact Netsafe to get further advice:

- **Website** - www.netsafe.org.nz
- **Text** - 'Netsafe' to 4282
- **Email -** help@netsafe.org.nz
- **Call -** 0508 NETSAFE (0508 638 723) The helpline is open from 8am to 8pm Monday to Friday and 9am to 5pm on weekends.

If you are still concerned, please talk to your People Leader or the HSS team who will be able to advise on next steps. See also next section: Escalating and reporting digital internally.

7. Escalating and reporting digital harm internally

The scenarios below provide information on immediate steps our staff and contractors must take upon identifying or receiving a harmful digital communication.

Communication scenarios	Escalation
Threatening communication: • published on a social media platform; • sent directly to staff, contractor (for example, personal phone, work mobile, personal email, contact at home address) • uploaded to Kāinga Ora online platform, such as MyKāingaOra	• Assess and escalate in accordance with Kāinga Ora Threat Management Process • See Internal escalation section for actions required
Offensive communication: • published on social media platform • sent directly to staff, contractor • uploaded to Kāinga Ora platform, such as MyKāingaOra	• See Internal escalation section for actions required
Communication published to social media platform that: • identifies individual staff or contractors by name, image and/or recording	• See Internal escalation section for actions required

• releases sensitive information about a staff member or contractor, such as a phone number or home address	

Internal escalation

If any threatening, harmful or disturbing content is sent:

- report it immediately to your People Leader/Manager
  Note: If the content is disturbing or harmful, do **not** share the actual content with the People Leader (this is to protect them from also being distressed by the material) just tell them what has happened; then
- notify the Senior Security Advisor by emailing securitypriorityevent@kaingaora.govt.nz so that they can assess and mitigate risk and provide support as needed; and
- report in Noggin and Kotahi (if tenancy related).

Note:
See also Raising a work order from MyKaingaOra SRQ if harmful content relates to MyKaingaOra.

8. Supporting your wellbeing

It can be distressing reading harmful comments about yourself or your work online.

As well as reporting the content it's important that you seek support if your wellbeing is impacted. Talk to your People Leader if you are concerned and discuss support options.

Your People Leader and the Health, Safety and Support team are here to help you. Please report concerns you believe we should be aware of.

If you are aware of a post on a social media platform that has an impact on your health, personal security or mental wellbeing, please report this using the Noggin 2 Incident Reporting System as soon as possible.

For other online related concerns, you can also reach out to the Technology Security and Risk Team at Kāinga Ora. While they are not social media experts, they can assist in providing guidance where possible.

Our Employee Assistance Programme

You can access the Employee Assistance Programme (EAP) for voluntary, private and confidential counselling services. Contact EAP on 0800 327 669 (0800 EAP NOW) or speak with your People Leader or Senior Advisor Health and Wellbeing for more information about support options.

9. Help

If you require help or information about this guidelines, please contact the Health, Safety and Security Team for assistance.

10. Document control

Details of previous versions of this document will be stored in our document management system (Objective).

Version	Reason for change
1	This guideline replaces 'Social media safety – Guide for our team member' (originally authored by Jayson Kingsbeer who no longer works for Kāinga Ora), which is archived.

SME review

Name	Designation	Date
Shaun Veenswyk	Health Safety Security Coordinator	10/6/2021
Alexa Zelensky	Social Media Advisor	9/6/2021
Naomi Hosted	Manager Technical Response	10/6/2021

Endorsers

Legal		
Juliet Philpott	Solicitor	21/06/2021
Business owner		
Tarniya Comrie	Director Safety Support and Wellbeing	22/06/2021

Keywords for Atamai

SSGDL003; SS-GDL-003; Social media harassment; online safety; how to deal with online abuse; Facebook; YouTube; Twitter; Instagram; Social media safety; how to deal with social media abuse; How to report social media content

Information architecture

SS Support Safety and Security - Manage Health Safety and Security > Guidelines > SS-GDL-003