17/241/7

28 February 2017

David Johnston
fyi-request-5352-67f0538a@requests.fyi.org.nz

Dear Mr Johnston

I refer to your email of 9 February 2017 in which you requested *'the latest documentation regarding NZ Police guidelines/requirements for employee's use of social media.'*

I have considered your request in accordance with the Official Information Act 1982. I **enclose** a copy of the requested information. Please note that some details have been withheld pursuant to section 9(2)(a) of the Official Information Act 1982 to protect the privacy of natural persons.

Yours sincerely

Jane Archibald
Acting Deputy Chief Executive: Public Affairs

Social Media Policy

Detailed table of contents

This chapter contains the following topics:

Executive summary

Police has a strong social media presence across all of the major social media platforms. This policy will help to guide you when using work and personal social media, disseminating messages on Police accounts, and interacting with our followers.

The Code of Conduct applies to all employees when using social media (both for work and personal purposes). It is also crucial that personal and work social media activity remains separate. Be aware of the risks of using social sites and take the steps below to protect yourself, your (and our) reputation, your family, colleagues and the wider organisation.

If any of the above criteria are not met, administrations rights may be removed or pages closed down. The Police social media approach is intended to be responsive, engaging and representative of our brand. Adhering to these guidelines will ensure we have a consistent and positive online presence.

Police social media contacts

- [redacted]
- [redacted]

Personal use of social media

Dos

- When posting personal opinions on your personal social media accounts, make sure that it's clear that it is your own view and not the Police view on a particular issue.
- Only access personal social media sites at work as outlined in the 'Information management, privacy and assurance' chapter in the Police Manual.
- Select high privacy settings on your personal accounts to prevent others (including media) viewing or using your information and photos.
- Be aware of security advice issued through the Bulletin Board – do what you can to avoid being the victim of harassment, identity theft, or other unwanted attention from criminals.

Don'ts

- Don't use personal profiles for any work related activity including posting information and/or work related images (including images in uniform).
- Don't use your personal email address or phone number for Police social media accounts.
- Don't post anything that can bring Police into disrepute or negatively impact the reputation of Police (i.e. anything in breach of our Code of Conduct).
- Don't post anything that compromises your security or the security of family or colleagues (e.g. posting personal information such as phone numbers or addresses).

Work use of social media

Social media helps Police promote a sense of community, collect information, share crime prevention advice, gain information on wanted people, and receive feedback. However, the same rules apply to social media as to any other method of receiving and imparting information on behalf of Police.

Dos

Policies and guidelines

- Be aware of, and comply with, the Police media policy.
- Be familiar and comply with Police instructions that apply to traditional communication methods as these also apply to communication via social media:
  - Releasing information to the media
  - Community disclosure of offender information
  - Sub judice
  - Wanted persons postings
  - Photographs of shop thieves
  - Missing persons
  - Crime Prevention Cameras (CCTV) in Public Places

Page use

- PNHQ Public Affairs (via [redacted]@police.govt.nz) must have admin rights to all Police related pages/social media accounts to ensure every Police page meets Police's standards, to post on behalf of Districts (for operations and to post wanted and missing people etc.) and to manage campaigns and project work
- Seek permission from the National Manager Brand and Engagement before creating any new social media accounts on any of the available platforms – Twitter, Instagram, YouTube, Google+, LinkedIn, Snap Chat etc.
- Be aware of, and take steps to manage risks of:
  - loss of control over data and images
  - identity fraud and fake accounts
  - viruses, hacking and unauthorised access to Police accounts
  - creating an electronic footprint (in covert settings).
- Follow the social media guidelines and maintain and monitor sites daily. The public are entitled to express their own opinions, but messages that are obscene, offensive, or in breach of the platform terms and conditions should be hidden or removed. People who post offensive material should be blocked from using the site.

Content and private messaging

- Ensure that all legitimate private messages (spam excluded) are responded to as quickly as possible. Police's expectation is that all messages will be responded to within 2 hours.
- Ensure that your page/account is free from any hate speech, dangerous or misleading communication or instances where an individual's privacy is breached.

Branding and imagery

- Ensure the social media account you're managing uses Police's current branding/corporate ID and appropriate imagery. Approach the National Manager Brand & Engagement (in Public Affairs) if you'd like assistance.

Privacy

- Comply with the Privacy Act 1993. Do not post personal information online without the individual's consent unless it is necessary for a police function (such as trying to locate an offender, or identify a person in an image for the purposes of an investigation). Make sure anything posted is accurate (and not misleading) and up to date.

- Treat information received through social media in the same way as you treat information provided through traditional channels. For example, make sure it is stored appropriately, and retained (or disposed of), in accordance with the Privacy Act 1993, the Public Records Act 2005, the Criminal Disclosure Act 2008, and the Police records management policies.

Don'ts

- Don't post content that could conflict with our organisational messaging, operating style (e.g. when speaking to members of the public in person we always treat them with respect and aren't sarcastic or mocking etc. – the same applies online) or bring Police into disrepute. All content must be politically neutral.
- Don't create any new Facebook pages. To minimise risk to the public and to ensure Police delivers a consistently high quality of service, Police's Facebook presence is limited to one page per District, a Police Museum page, Recruitment page and National New Zealand Police page. Any additional Facebook pages will be merged with one of these pages. If you wish to create a new social media page on any other platform, please seek permission from National Manager Brand & Engagement (Public Affairs).
- Do not engage in argumentative or aggressive discussions with users on Police social media pages. Such discussions can have a detrimental effect on the NZ Police brand and reputation. Comments with profanities and bad language will be automatically hidden by Facebook's page moderation function. Negative comments can be manually hidden from our pages if needed.
- It is expected that all Police responses to questions and comments (including provision of advice and guidance) will have a positive and supportive tone. If you are unsure how to interact or respond to comments on any of the Police social media pages, please contact [redacted].

Using social media for overt and covert investigations

When using social media overtly in an investigation, requests for information can be made directly to the social media organisation. Staff can also consult the National Cyber Crime Centre (NC3) on [redacted] - **number not for public use**.

If you are using social media covertly in an investigation you must obtain the approval of the National Criminal Investigations Group at PNHQ. Please read the 'Covert telecommunications' section in the 'Covert backstopping' chapter for more information.

Social media may be used for other purposes, such as negotiating or to spread reassurance during tactical operations. Before doing so, contact the appropriate business group for advice:

- For negotiations, contact your local Police Negotiation Team.
- For tactical operations, contact the Media Centre.