NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

16 May 2022

Michael Junior

Fyi-request-xxxxxxxxxxxxxx@xxxxxxxx.xxx.xxx.xx

REF: IR-01-22-11011

Dear Michael

I refer to your email of 18 April 2022 where you requested under the Official Information Act 1982 (OIA) the following:

1. *Is a policeman allowed to take an email address he obtained as a policeman and put that email address in the public domain and encourage people to send emails to the email address he published on-line?*
2. *Where a policeman receives an email to his police email address is he allowed to take that email address he received an email from and send the person an email from his personal email address?*
3. *Are either of the above actions something Police would investigate if the victim notified police that both of these things happened?*
4. *Under any police rules, guidelines or policy's would a senior policeman who was notified of both of the above incidents be obliged to take action or are they allowed to ignore the notification?*
5. *Can I have a copy of any police rules that are about social media and the public domain as well as information a policeman gets through police sources or their police email address.*

In response to your first two questions, every Police employee has a 'work' email address. Limited personal use of Police technology, including the email system, is permitted but must at all times be consistent with Police values and the standards of behaviour expected of an employee. In addition, personal use must be kept to a minimum so that official duties are not compromised. Without knowing the specifics of what you have set out in question 1, it is difficult to assess whether this behaviour fits within the acceptable guidelines.

It is difficult to answer question 3 without knowing the specifics of what has allegedly occurred. However, we would always encourage anyone who has concerns about the conduct of a Police employee to notify us about their concerns. This can be done in a number of ways, including through the Police website at the following address: https://www.police.govt.nz/contact-us/give-feedback-about-police. Alternatively, someone can contact their local Police station during opening

Police National Headquarters
180 Molesworth Street. PO Box 3017, Wellington 6140, New Zealand.
Telephone: 04 474 9499. Fax: 04 498 7400. www.police.govt.nz

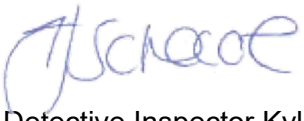
hours to lodge a complaint or call 105. Anyone can also complain to the Independent Police Conduct Authority (IPCA) at https://www.ipca.govt.nz

To answer question 4, if Police receive a complaint then the complaint must be notified to the IPCA pursuant to s.15 IPCA Act 1988. Any action taken will depend on the nature of the allegation and will be determined in conjunction with the IPCA.

I have attached a copy of the Police Social Media Policy. This has been redacted pursuant to s.9(2)(a) of the OIA to protect the privacy of natural persons. Furthermore, internal email addresses have been redacted pursuant to s.9(2)(g)(ii) of the OIA to maintain the effective conduct of public affairs through the protection of such Ministers, members of organisations, officers, and employees from improper pressure or harassment.

You have the right, under s.28(3) of the OIA, to ask the Ombudsman to review my decision if you are not satisfied with the way I have responded to your request.

Yours sincerely



Detective Inspector Kylie Schaare
Acting Director: Integrity and Conduct
New Zealand Police

Police Instructions

Social media policy

Policy statement and principles

What

Police have a strong social media presence across several major social media platforms. This policy will help to guide you when using work and personal social media and interacting with our online communities. The policy also references other Police policies and guidelines that support it, as well as specific social media features and functions that have an important role in providing guidelines for staff.

Why

Media & Communications are responsible for setting the strategy for social media and day-to-day management of all accounts. The Police social media approach is intended to be consistent, responsive, engaging and representative of our brand. Adhering to these guidelines will ensure we have a consistent and positive online presence that supports Our Business and increases public trust and confidence. Content that does not adhere to this policy may be hidden, removed or escalated for learning and resolution.

How

The Code of Conduct applies to all employees when using social media (both for work and personal purposes). Be aware of the risks of using social sites and take the steps outlined to protect yourself, your (and our) reputation, your family, colleagues and the wider organization.

Police social media contact

s.9(2)(a) OIA

For any queries related to social media, please email s.9(2)(g) OIA

Our social media platforms

Media and Communications monitor social media trends and makes

strategic decisions as to which platforms suit our engagement needs.

As part of the Police Social Media Strategy this is our current social media presence.

	National Page	**District Pages**
Facebook	Yes	Yes
Twitter	Yes	No
Instagram	Yes	Yes
LinkedIn	Yes	No
YouTube	Yes	No
Neighbourly	Yes	Yes

Our national Facebook pages are New Zealand Police, NZ Police Recruitment, and NZ Police Museum.

Twitter: In addition to the national NZ Police account we also have an NZ Police Media account which is an RSS feed of media releases for journalists and a Commissioner of Police Twitter account, which is managed by Media & Communications.

TikTok: We have a verified account, but we do not post content on it. There are guidelines in place, however, for staff regarding personal use of TikTok. Click here to see the guidelines.

Our social media model

To ensure a consistent, manageable and professional online presence, the Police social media model is limited to one Facebook & Instagram page per district, as well as the set national pages. Rather than having multiple pages per district, ours is a district model. We have one district page, and we communicate through that page.

Our policy is based around investing most of our time in Facebook and Instagram, as these channels have the highest levels of engagement and reach our target audience the best.

New accounts must not be set up without making prior contact with Media and Communications, PNHQ – email: s.9(2)(g) OIA

Community guidelines and appropriate commentary

We encourage contributions to the pages, however any comments that are deemed inappropriate or in breach of a social media platform's terms and conditions will be removed.

We have community guidelines in place to help create a safe environment on official New Zealand Police social media channels.

We welcome questions and commentary, including constructive feedback and differing opinions, however, please ensure comments are relevant and respectful.

As per the Community Guidelines:

New Zealand Police reserves the right to:

- determine what constitutes inappropriate content
- edit or entirely remove inappropriate content, and
- ban users from its social media communities.

We may delete posts that are:

- racist, sexist, homophobic or other forms of hate-speech
- potentially defamatory
- spam, or

that contain:

- offensive language, abuse or threats
- off-topic or irrelevant information to the thread of conversation
- nudity, pornography or child abuse

- excessive violence
- content that is illegal, gives instructions for illegal activity or advocates illegal activities
- personally identifiable information.

Here are our the Community Guidelines. These are available to the public on our website and linked via our social channels.

We operate an extensive profanity filter in the backend of our pages. If a word you believe should be banned is coming through, please email s.9(2)(g) OIA and let us know. When a word in the filter is used, the comment will be automatically hidden. Hidden comments are only visible to the original poster and any of their connections.

Comments can be turned off for posts made on Facebook and Instagram. Comments will be turned off only in situations where most of the commentary is expected to, or does, breach our community guidelines. Comments will always be turned off on Wanted to arrest posts.

Personal use of social media for staff

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 security' chapters 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 Pānui. Do what you can to avoid being the victim of harassment, identity theft or other unwanted attention from criminals.
- Do report any content of concern regarding staff members or Police to s.9(2)(g) OIA

For more information on keeping yourself safe online, go here.

If you see something inappropriate posted by a staff member, please raise it with s.9(2)(g) OIA

Don'ts

- Posting photos of yourself in uniform on personal social media accounts, or anything that identifies you as a Police officer is not recommended.
- 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/safety of family or colleagues (e.g. posting personal information, such as phone numbers or addresses).

Other relevant NZ Police policies and guidelines

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
- Missing persons
- Crime Prevention Cameras (CCTV) in Public Places
- Filming Operations Policy
- Police media policy.

Content and moderation

Responsibility for day-to-day management of the accounts, including content creation, posting, monitoring and moderation sits with the social media team at PNHQ.

For non-urgent post requests, or to submit content from your district, please email s.9(2)(g) OIA All content submitted must have the appropriate permissions granted (as per this policy) from those pictured and/or involved.

For urgent posts, the social media team is available between 8.30am and 5.00pm weekdays (excluding public holidays) – please contact s.9(2)(g) OIA

Outside of these hours, the media team will handle genuine, urgent operational requests, such as crashes or Wanted to arrest posts. The media team can be reached at s.9(2)(g) OIA . All comments on Wanted to arrest posts will be turned off. Any non-urgent requests sent to the media team will be pushed back to the social media team.

Private messaging through Facebook

Private messaging functionality is turned off for some Facebook pages, while for some it is still on.

For those pages that private messaging is still on, messages (spam excluded) are responded to as quickly as possible. **All messages need to be responded to within 24 hours.** Private messaging is managed by the social media team at PNHQ.

Wanted to arrest posts

In relation to 'WTA' posts, the following process must be followed:

- there must be urgency – the person wanted must be considered a risk to staff or the public and apprehending them is a matter of urgency
- consideration must be given to the likelihood of the photograph encouraging trolling – will the photo result in negative/bullying commentary?
- posts must be made in consultation with your DCC and with approval from the NCCC.

The decision to go public with a wanted photo must be a last resort, rather than a first step. An image of a person may only be posted if that person cannot reasonably be located by other means. Enquiries undertaken to locate the wanted person must have failed, and/or there are compelling reasons to publicise the image without delay.

Wanted to arrest posts should use only objective language to describe the person, and should **not** include any of the following:

- any other personal information (such as health status)
- reference to the person's ethnicity, unless this will materially aid in the person's identification
- indicate if the person has previous involvement with Police (e.g. PRN)

To submit a wanted post:

1. District staff send their wanted post request to their DCC (using the approved template below)
2. If the DCC agrees the request meets the criteria above, the DCC forwards the wanted post request to s.9(2)(g) OIA

3. NCCC assess the request and, if approved, send it to s.9(2)(g) OIA for copywriting with nationally consistent wording.
4. If within 8.30am–5pm, the media team will forward to the social media team for posting. Any requests outside these hours will be posted by the media team and forwarded to the social media team for reference only.
5. The post will be made with comments turned off.

Simply copy/paste the below template and attach the NIA image to submit for approval.

For district completion:

Offender (LAST NAME/First Name):	
PRN:	
File no:	
District Facebook page for posting:	
How does this person meet the threshold:	*Please include specific details about their risk level and urgency, as per the policy.*
Post request by (name + QID):	
District sign off (name + rank):	

For NCCC completion:

Does this post meet NZP social media policy threshold:	Yes / No
Reviewed by:	

Once a person has been apprehended, s.9(2)(g) OIA (or s.9(2)(g) OIA if outside business hours) must be notified as soon as possible so the post can be removed.

Missing persons

All missing person/s posts must be approved by the supervisor of the person making the request.

Once approved, the request should be made to the media team who will write nationally consistent wording and pass to the social media team for posting. If outside business hours, the media team will post.

Posts should use only objective language to describe the person, and should not include any of the following:

- any other personal information (such as health status)
- reference to the person's ethnicity, unless this will materially aid in the person's identification
- indicate if the person has previous involvement with Police (e.g. PRN)

The district staff member making the request must ensure the family are aware of the post and concerns addressed – the necessity of the post should be explained to the family.

Once the person has been found, the media team and s.9(2)(g) OIA must be notified as soon as possible so the post can be removed.

Persons sought

All person/s sought posts must be approved by a senior person within district (as listed below).

District approvers must be one of the following: Detective Inspectors, Detective Senior Sergeants, Area Prevention Managers; DCC Shift Managers; ISU Senior Sergeant; District Intelligence Manager and any District Intelligence Supervisors.

Once approved, the request should be made to the media team, who will write nationally consistent wording and pass to the social media team for posting. If outside business hours, the media team will post.

Posts should use only objective language to describe the person, and should not include any of the following:

- any other personal information (such as health status)
- reference to the person's ethnicity, unless this will materially aid in the person's identification
- indicate if the person has previous involvement with Police (e.g. PRN).

Once the person has been found and/or identified the media team and s.9(2)(g) OIA must be notified as soon as possible so the post can be removed.

Lost and stolen property

To regulate the amount of posts regarding property that's lost, found or stolen, posts will only be made for items assumed to be of significant sentimental value e.g. engraved jewellery, or of monetary value exceeding $300. Items such as cell phones and keys will not be posted.

Use of content regarding youths

Using imagery and video content of people under the age of 18 requires permission from a parent/guardian. We must not post any content showing youths related to anything illegal, potentially illegal, or anything that could cause harm to the person(s) in question, should they be identifiable. If in doubt, check with your district legal staff. In these circumstances, no person under the age of 18 should have their image or video posted on any of our social media pages (even with a blurred image).

The main exception to this would be when the person in question is a high risk (to the community or themselves), finding them is of an urgent nature and all other options have been exhausted. Even in these cases,

the person should be ‘sought’ rather than ‘wanted’ and without reference to why they are sought. In these situations, the need to post must be signed off within district.

District approvers must be one of the following: Detective Inspectors, Detective Senior Sergeants, Area Prevention Managers; DCC Shift Managers, ISU Senior Sergeant; District Intelligence Manager and any District Intelligence Supervisors.

Genuine (a matter of urgency) missing person posts can of course be made for people under the age of 18 with consent from a relevant parent or guardian.

Filming guidelines for social media

When filming (video) for social media use, there are a number of guidelines and risks associated with this kind of content – some due to legal requirements, some due to NZ Police Policy, and some based on best practice (and what can be expected in the social media environment).

Please follow the Social media filming guidelines. These guidelines are largely based on information from Response & Operations, Legal, and our reality TV involvement

Live streaming

Live streaming is not used as a tool for day-to-day engagement with followers. This is because Police have no ability to moderate live streaming posts, therefore still imagery and pre-recorded video is the preferred engagement option.

There may be specific occasions or approved Police events where Facebook live can be used, but you must get permission in advance from the Marketing & Brand Manager (s.9(2)(a) OIA).

In general, live streams will only be considered for events such as:

- high profile media conferences on a major critical incident involving Police
- high profile national events, e.g. significant award ceremony, graduations and Remembrance Day.

Use of music and soundtracks

Any music use in social media videos (or any video, in fact) needs to be royalty free or have copyright clearance from the producer of the music. Getting permission for the use of (well-known and recognisable) music is likely to be expensive and will be a timely process. Use of music without permission from the publisher can result in legal outcomes.

We have a paid subscription to Artlist and can get you music for videos if/when required.

Use of imagery

Any imagery used that is not owned by NZ Police must always have permission for use from the owner of the image (including staff and members of the public). Alternatively, the image needs to be purchased from a licensed agency (e.g. Gettys). Wherever possible, however, we should always use images with the Police brand/identity – purchasing images should not be required often, due to the stock of our own imagery we have available.

Branding and tone of voice

Branding, imagery and tone should be consistent, and as outlined in the Brand Style Guide and Social Media Strategy. Items such as profile pictures, auto replies, usernames and any other settings should only be by edited by the PNHQ social media team.

It is expected that all Police responses to questions and comments (including provision of advice and guidance) are positive and supportive. Interactions online should be respectful – never sarcastic or argumentative.

Posts should not be attributable to individual staff members, this ensures the longevity of accounts, protects staff privacy, and builds the NZ Police brand.

Posting photos of Police employees

Verbal consent must be sought before posting photos of Police staff on Police social media accounts. Check that consent has been given by staff before sharing new social media posts featuring Police employees.

Posting photos of the public

Verbal or written consent must be sought before posting photos of members of the public on Police social media accounts. There are talent forms available – email s.9(2)(g) OIA

Privacy

- Comply with the Privacy Act 2020. 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 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 2020, the Public Records Act 2005, the Criminal Disclosure Act 2008, and the Police records management policies.

Politically neutral/areas for comment

- Avoid posting content that could:
  - conflict with our organisational messaging
  - provide comment on national policies or our operating model
  - bring Police into disrepute
- All posted content must be politically neutral.

Using social media for overt and covert investigations

Social media provides useful open source intelligence. You can:

- confirm identities
- identify aliases
- identify associates
- identify vehicles
- identify locations of interest
- identify criminal offending.

Do not use personal social media profiles to contact witnesses or to search offenders' accounts. Please email s.9(2)(g) OIA if you wish to make contact with a member of the public via social media. This is only to be done as an initial means of contact and should be a last resort.

High Tech Crime have developed some best practice around conversing with members of the public where Facebook is the only means of contact. If you would like more information about this, please email s.9(2)(g) OIA .