Te Tari Pūreke
Firearms Safety Authority

2 March 2026

IR-01-26-4256

s 9(2)(a) OIA Privacy

Tēnā koe s 9(2)(a) OIA

Thank you for your Official Information Act 1982 (OIA) request dated 6 February 2026. I have answered each of your questions below:

> *If the authorisation was given to send a bulk email out to every single license holder that is on the FSA's records, would the regulator, as of yesterday, have the capability/infrastructure to send that email in bulk?*

Yes, the Firearms Safety Authority (the Authority) use a tool called Enudge for sending bulk emails.

The Enudge bulk email service is managed under an enterprise subscription licence, providing a dedicated tenant for the Authority and New Zealand Police. This means the New Zealand Police Enudge product resides in a separate tenancy from other Enudge customers. A thorough security risk assessment was undertaken by New Zealand Police as part of the certification and accreditation process prior to the implementation of the product and service.

> *How quickly could a notification of this nature be sent to every firearm license holder's email address held in the FSA's database? Does the FSA have a SOP for bulk notification of license holders via email, if so, please include this SOP document in your response.*

The Authority can set up a bulk email for sending within hours, provided the formal approvals are given at the correct stages. Please refer to the attached SOP document.

> *If not mentioned already by the above questions, can you also please highlight examples of when a bulk message would be sent out to license holders.*

Any time there are more than ten people who need to receive the email. For example, bulk emails have been sent out for changes in legislation (Clubs and Ranges, Dealer changes i.e. ammo selling requirements), reminders for licence expiries and reminders for Firearms Registry responsibilities.

Would a scenario such as raising awareness on how to submit on regulatory consultation, and firearms-related Bills be included.

To date, we have used the email sent to all licence holders in our database to advise them about imminent changes in regulations that would be impacting them. For example, when the Firearms Registry was introduced, we messaged licence holders after the Regulations were Gazetted, with what licence holders would have to do from 24 June 2023 onwards.

We have not used bulk emails to advise licence holders of things that may just be of interest to them generally. For example, previously consideration has been given to using the ability to email all licence holders to share messaging to build confidence in the Firearms Registry (at a significant milestone) and to clarify issues around filling in the Registry that licence holders were saying were causing them difficulty. Advice received at that time was that using this channel in such a way did not appear to be consistent with the reason licence holders' emails had been collected.

This advice was accepted and has driven the approach to the use of bulk emails to all licence holders since. Not using the bulk email to raise awareness about the consultation period for the Arms Bill is consistent with this accepted setting. That is, informing licence holders of the progress of a Parliamentary process does not appear to meet the established threshold for use of this channel.

The use of emails to all licence holders will likely be reviewed after the passing of the new Arms Bill. This is because when enacted, this Bill sets up the new independent regulator. It will likely become clearer from then what the Government intends the Authority's regulatory purpose to be. This may widen the scope for providing regular informative messages to licence holders via bulk email, if such emails are determined to be consistent with the purposes of the new regulator.

If not already mentioned, what would the process for approval of a message to be sent out require, and would the content of this message require approval from the Police Commissioner?.

Please see attached SOP document which outlines the process however, depending on the message being sent it would require approvals from different levels, generally the highest authority for approval is the Executive Director of the Authority.

You have the right to ask the Ombudsman to review this decision if you are not satisfied with the response to your request. Information about how to make a complaint is available at: www.ombudsman.parliament.nz.

For your information, Police has developed a process for proactive release of information, so the anonymised response to your request may be publicly released on the New Zealand Police website.

Nāku noa, nā

Natalie Williams
Acting Director – Partnerships & Communities, Strategy, Performance and Capability
Firearms Safety Authority

Te Tari Pūreke email policy

Table of Contents

Table of Contents 2

Policy statement and principles 3

- What 3
- Why 3
- How 4

Overview 5

- Introduction 5
- Legislation governing information 5

Out of Scope

[redacted]

Sending emails externally to members of the public 10

- Sending an email to a single external recipient: 10
- Sending an email to multiple external recipients (Enudge) 10

Out of Scope

[redacted]

Policy statement and principles

As a government agency, Police and Te Tari Pūreke follow the Government's minimum security requirements defined in the Protective Security Requirements (PSR) and the NZ Information Security Manual (NZISM).

The PSR outlines the Government's expectations for information, physical and personnel security. The NZISM details processes and controls representing good practice essential for the protection of Government information and systems.

We all ensure information is only collected, accessed, used and shared for authorised purposes, is kept secure across all environments and is managed in accordance with applicable legislation such as the Public Records Act 2005 and the Privacy Act 2020.

What

This chapter outlines the additional email requirements for Te Tari Pūreke (a business unit of New Zealand Police) staff.

The underlying requirements are outlined in the Police Information Security Police Instructions chapters.

Why

Information held by Police and Te Tari Pūreke must be:

- only accessed if there is a legitimate need to do so, especially if it is personal information
- handled carefully, especially when it is being carried or sent outside Police premises
- released only in accordance with legislative requirements, directives of Government or Courts, or in accordance with Police policy.

Te Tari Pūreke handles sensitive information in relation to firearms licence holders, licensed dealers and persons with access to firearms. Staff must exercise extra caution when sending emails externally as:

- the path or destination may not be secure
- sending emails to non-Police addresses increases the risk of them being intercepted or received by a third-party
- sending emails containing personal information to the wrong recipient is a privacy breach.

Sending emails to the wrong people with private, personal or sensitive content can cause significant downstream problems.

In the firearms licence context, sending licence holder information to the wrong recipient or to an insecure email address may jeopardise sensitive licence holder information and threaten public safety if the licence holder's information is then used for nefarious or criminal purposes.

For this reason, it is important for Te Tari Pūreke to have additional steps and policies in place for

sending emails.

How

By having rules for sending emails and being aware of the risks when sending emails, Te Tari Pūreke will better protect the community, firearms licence holders and licensed dealers, and the trust and confidence in NZ Police.

Any privacy breach or near miss privacy breach, no matter how big or small must go through the privacy breach management process. The Privacy team at PNHQ can be contacted for advice if needed.

The Code of Conduct also applies as all Police and Te Tari Pūreke staff are required to follow the organisational policies under the Code of Conduct.

Overview

Introduction

This chapter covers the steps Te Tari Pūreke staff must take when:

- setting up their Outlook email inbox and any shared email inboxes (email settings)
- sending emails internally to Police staff and other [SEEMAIL] government agencies
- sending emails externally (to members of the public).

Legislation governing information

The key legislation governing information use and management is:

- under section 50 of the Policing Act 2008, a person commits an offence who without lawful authority or reasonable excuse, has in their possession any Police property, including any confidential Police document
- the Privacy Act 2020 mandates protection of personal information about any person. The Privacy Act establishes principles relating to the collection, storage, use and disclosure of information relating to individuals
- the Official Information Act 1982 applies to all requests made to public sector agencies for information that is not about the requestor.

Out of Scope

Out of Scope

Out of Scope

Sending emails externally to members of the public

All Te Tari Pūreke staff must follow the below steps when sending emails externally to members of the public (non-Police and non-[SEEMAIL] government agencies).

The steps are separated into:

- Sending an email to a single external recipient
- Sending an email to 10 or more external recipients

Sending an email to a single external recipient:

1	Password protect documents	This is a requirement for all documents being sent to a non-Police email address. The password protection guide is available here.
2	SELF-CHECK	Apply the SELF-CHECK tool
3	Check recipient(s), content and attachments	The sender must double-check that the recipient's email addresses are correct, the content (body) of the email is correct and intended for the recipient and all attachments are password protected.
4	[SEEMAIL]	When sending an email externally, [SEEMAIL] must only be removed after the above steps have been completed.

Once the above steps are completed, the email may be sent.

There is no limit to how many individual emails are sent by staff to single external recipients. However, if the same email is intended for 10 or more external recipients (for example a generic licence expiry reminder email), staff should follow the process for 'Sending an email to multiple external recipients (Enudge)'.

If there is any doubt about the steps above, the content of the email or the recipient, or whether the Enudge tool should be used, staff should consult with their supervisor or manager.

Sending an email to multiple external recipients (Enudge)

Enudge is a tool used to send individual emails to multiple external recipients in an efficient and safe way. It is recommended that staff use the Enudge option if they intend to send the same email to more than 10 external recipients.

For clarity, if sending the same email to less than 10 external recipients, the emails must be sent individually per the instruction under "Sending emails to a single external recipient"

1	Seek pre-approval from manager to use Enudge	Staff should discuss using the Enudge tool with their supervisor and/or manager before completing the steps below.
2	Complete request template	The request template is available here: TTP_Bulk_Email_Approval_Template.msg For instructions on adding the template for use on a regular basis within Outlook follow this instruction: Outlook Stationery.pdf
3	Attachments	Attachments are not available for use within the bulk email tool.
4	SELF-CHECK	Apply the SELF-CHECK tool
5	Supervisor review	Supervisors should check the template has been completed correctly, satisfy themselves the recipients' email addresses are correct, and that the content (body) of the email is correct and intended for the recipient. The request can then be sent to manager for approval.
6	Manager approval	Managers can approve their staff member's request by responding with "approved" once they have checked the template, content, and recipients list. Managers may refuse the request.
7	Send to processor	If approved, forward the approved email thread to the contact person listed on the 'TTP Bulk Email Approval Template'

Out of Scope

Out of Scope