



Headquarters
New Zealand Defence Force
Defence House
Private Bag 39997
Wellington Mail Centre
Lower Hutt 5045
New Zealand

OIA-2026-5889

17th August 2026

[REDACTED]
[REDACTED]

Dear [REDACTED]

I refer to your email of 20 July 2026 requesting, under the Official Information Act 1982 (OIA), the following:

1. *Please provide the NZDF's current policy, guidance or instructions relating to the use of Strava, fitness-tracking applications, GPS-enabled wearable devices or location sharing by NZDF personnel.*

Defence Force Instruction (DFI) 60.20 Acceptable Use of Digital Systems and Devices is the policy regarding New Zealand Defence Force (NZDF) owned or leased digital systems of the Defence Information Environment, and any digital devices in any location that are used to conduct NZDF functions. There is no policy specifically concerning the use of *Strava, fitness-tracking applications, GPS-enabled wearable devices or location sharing*.

DFI 60.20 provides the following general provisions:

- All users are accountable and responsible for their actions when using NZDF resources. Users will be held accountable in any situation where their behaviour or actions could impact on the operation of the NZDF, or its reputation.
- Users are responsible for ensuring their behaviour is appropriate and acceptable within their operating environment.
- Users of digital systems and devices need to apply good personal judgement and consider legal, security, productivity, and ethical impacts of their actions. Users who are NZDF personnel also have a duty to act in a manner consistent with the core values of the NZDF.
- Unacceptable use and behaviour includes, but is not limited to, activity that—
 - (1) breaches any law (including the Privacy Act 2020, the Copyright Act 1994, the Trademarks Act 2002, and their counterpart laws in other countries);
 - (2) creates unnecessary security risk around assets, people, operations, capabilities and/or information;
 - (3) creates a loss of productivity, for example, electronically transferring games, downloading video files, sending spam, personal advertising, or any other forms of mass emailing except for authorised notices;
 - (4) interferes with work or official duties, such as day-to-day work or operational readiness;
 - (5) divulges NZDF network information (unless there is a need to share network information for legitimate business purposes). For example, sharing Internet Protocol (IP) addresses, server names, detailed descriptions of installed software which includes versions and/or

patch status, details of any security software or hardware elements including product names to anyone without a legitimate business need to know.

At enclosure one is an extract from the NZDF Social Media Handbook that provides guidance on the use of fitness trackers and applications.

2. Please provide any advice guidance or instruction issued following the January 2018 Strava Global Heatmap reports.

The below guidance was provided by Defence Security to NZDF personnel. Where indicated, specific advice is withheld in accordance with section 6(a) of the OIA as it relates to particular security concerns.

18 May 2020

Investigations website Bellingcat has identified extensive vulnerabilities in a beer rating app called Untappd, similar to the vulnerabilities found in Strava fitness apps. Offering social network functionalities, the app can be mined for users' geo-locations, imagery, and social connections. This can reveal associations between app users and sensitive or restricted locations, potentially circumventing security measures in the app that prevent direct searches for military and intelligence community facilities. Bellingcat demonstrated how military and intelligence personnel have been identified and tracked, and their profiles exploited to discover information regarding their engagements, locations, and links to other military personnel.

There are serious security implications associated with the potential use of various social media apps offering searchable information about the user or their created and uploaded content. [section 6(a)]. NZDF personnel and contractors should limit and protect personal information and permissions granted to social media applications, and should avoid using apps that do not adequately protect personal information, or that could be used to identify sensitive NZDF roles, locations or movements.

June 2026

On 21 Mar 26, news media reported a French naval officer had inadvertently revealed the location of a French Navy Aircraft carrier by uploading his workout to the fitness tracking application Strava. This is not the first time Strava has been identified as a means of locating military assets and facilities. In 2017, Strava released a data visualisation map that showed all activity tracked by users of its application that allowed identification of military bases and base layouts around the world.

With the current global environment and rapidly enhancing personal technology, the threat of exposure online is higher than ever. NZDF personnel should be aware of their current exposure online. The recently released 'How Exposed Am I?' online tool from the New Zealand Government can help to show areas where enhanced online security may be required.

Public disclosure of NZDF information, unclassified or classified, increases personnel and the organisations vulnerability to targeting, including cultivation and exploitation, or cyber and physical security compromise. NZDF personnel are reminded that the sharing of NZDF information online, even at an unclassified level, should not be done. Another way to keep yourself safe online is to avoid joining groups that do not align with organisation values.

3. Since 1 January 2023, how many security incidents or investigations has NZDF recorded involving fitness-tracking applications or the inadvertent public disclosure of location information?

There are no reported security incidents concerning the inadvertent public disclosure of location information involving fitness-tracking applications.

You have the right, under section 28(3) of the OIA, to ask an Ombudsman to review this response to your request. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that responses to official information requests are proactively released where possible. This response to your request will be published shortly on the NZDF website, with your personal information removed.

Yours sincerely

GA Motley

Brigadier

Chief of Staff HQNZDF

Enclosure:

1. Extract from Social Media Handbook