DEFENCE FORCE INSTRUCTION 7.2
Official Information

Executive Series

Releasable to the public.

Office of the Chief of Defence Force
Headquarters New Zealand Defence Force
WELLINGTON

Authority Order

DFI 7.2
Official Information

Issued by the Chief of Staff, Headquarters New Zealand Defence Force

Authority

1. DFI 7.2 *Official Information* is issued and promulgated under the delegated authority of the Chief of Defence Force to the Chief of Staff, Headquarters New Zealand Defence Force.

Conflict

2. Nothing in this publication is to be construed as prevailing over any relevant Act of Parliament or regulations made under it, or Defence Force Orders and Directives issued by the Chief of Defence Force.
3. Any conflict between these orders and any other policy, order, direction or instruction issued within the New Zealand Defence Force is to be reported to the Custodian without delay.

AJ WOODS
Air Commodore
Chief of Staff HQNZDF
June 2020

Contents

Foreword

1. *DFI 7.2 Official Information* provides direction to members of the New Zealand Defence Force (NZDF) about the protection, availability, use and disclosure of information held by the NZDF. The instructions also address the requirement to retain and dispose of official information pursuant to the *Public Records Act 2005.*

2. The *Official Information Act 1982* (OIA) sets out the rules for responding to official information requests and is designed to hold Ministers and officials accountable for their actions in the course of their duties. Similarly, the *Privacy Act 2020* (PA) sets down a suite of privacy principles that must be adhered to when dealing with personal information.

3. As a nation, New Zealand has one of the world's most open and trustworthy governments. The NZDF is committed to improving how government responds to requests for official information. This includes making official information more accessible by adopting regular administrative practices for responding to requests for access to official information.

4. Leadership and a strong commitment to complying with the OIA and the PA are exercised from the very top of the NZDF. Successive Chiefs of Defence Force have set great value on providing access to official information. They have recognised that effective government relies on transparency and openness.

5. It is in the NZDF's best interests for the public to understand the work and achievements of the NZDF including the way in which it works to deliver on the organisation's responsibilities to the government and New Zealanders. In some cases contact between individuals working in the NZDF and the public can be achieved directly. In other cases, the media play an important role in facilitating this awareness and transparency. Nevertheless, such contact needs to be managed so that the professionalism and related reputation of the NZDF is not compromised. This publication sets out how contact with the media and other public communications are to be regulated throughout the NZDF by the implementation of good information handling policy and practice.

6. Effective compliance with the OIA and the PA means sustaining the right organisational structure to deal with requests for information, maintaining robust procedures and upholding an environment where executives, managers and commanders are fully aware of their responsibilities. Compliance with the OIA and the PA is not discretionary. At all times the NZDF approach to the provisions of these Acts is to meet all requests for official or personal information in accordance with the word and spirit of the Acts.

7. The Chief of Defence Force (CDF) places great emphasis on the security of personal information. CDF serves in a leadership role for privacy compliance and is accountable to the Government for implementing policies that enable consistent, effective privacy practices which minimise risk and ensure appropriate confidentiality of personal information including health information.

Preliminary Provisions

Purpose of DFI 7.2

1. These instructions state the New Zealand Defence Force (NZDF) policies and procedures for the management of official information and personal information including requests for access to that information in accordance with legislation, governmental direction and NZDF policies.
2. The setting of NZDF policies and procedures related to official information is intended to ensure that—
   (a) the NZDF complies with legislation and governmental policies; and
   (b) uniform conventions and standards for the protection and release of official information and personal information held by the NZDF are practiced.
3. The main component of these instructions—
   (a) state the mandatory requirements for the management and application of processes that control all aspects of providing access to official information and personal information throughout the NZDF;
   (b) detail the responsibilities for managing access to official information and personal information for eligible persons; and
   (c) prescribe the procedures and processes for dealing with requests for access to official information and personal information.
4. These instructions are consistent with guidance and direction from the Public Service Commissioner, the Ombudsman, the Privacy Commissioner and the Cabinet Manual. They implement the Chief of Defence Force's (CDF's) direction with respect to the use of official and personal information.

Application

5. This publication comprises general orders to members of the Armed Forces and instructions to members of the civil staff.
6. The instructions promulgated in this publication apply to all members of the NZDF and others engaged for NZDF purposes responsible for, but not limited to—
   (a) creating electronic and paper-based documents, media, publications, visual productions and web-based material;
   (b) the custody of official information and personal information;
   (c) responding to requests for access to official information and personal information; and
   (d) responding to general enquiries from ministers, the public and the media.
7. All members of the NZDF must comply with the policies and processes prescribed in this publication and ensure that their subordinates who may have access to official information and personal information in the course of their service or employment also act in accordance with the requirements.

8. It is the responsibility of the member of the NZDF managing any contractor, consultant, external service provider and any other person not a member of the NZDF to make them aware of these instructions.[1]

9. Non-compliance with these instructions may result in disciplinary action being taken in accordance with the *Armed Forces Discipline Act 1971* or may result in possible sanctions in accordance with the *NZDF Civil Code of Conduct*. Individuals who do not act to prevent incidents by others could be subject to the same measures. In the most serious cases this could ultimately lead to an individual being removed from an appointment, dismissed or discharged from the Service.

10. The directions and instructions in this Defence Force Instruction must be complied with except where significant circumstances allow for a properly authorised departure from the prescribed requirements.[2]

Commencement date

11. The commencement date of DFI 7.2 *Official Information* is 10 December 2020.

12. Amendments to this publication are documented in the Record of Change in the End Matter.

Repeal

13. The following orders, directions and instructions will be repealed by CDF Direction on commencement of this DFI—

    (a) *DFO 70 Defence Force Orders for Official Information;* with the exception of *DFO 70 Part 1, Chap 8 Protected Disclosures Act 2000* (which will be repealed at a later date);

    (b) *NZDP 0.70-2 New Zealand Defence Publication The Privacy Act 1993 – NZDF Procedures and Practices;*

    (c) *SADFO 10/2003*;

    (d) *SADFO 13/2006*; and

    (e) *SADFO 03/2015*.

Custodian

14. The Custodian of *DFI 7.2* is the Manager, Corporate and Ministerial Services, Office of the Chief of Defence Force.

[1] Any agreements under which such persons are engaged should be clear that information created in the course of performing the contract belongs to the NZDF and is subject to the *Official Information Act 1982* (OIA) in accordance with s 2(5) of the OIA.
[2] Authorising Authority is the Chief of Staff (CoS) Headquarters New Zealand Defence Force (HQNZDF).

Meanings of terms

15. Terms used in *DFI 7.2* and not explained or stated in the authorised references are defined in Annex A to these preliminary provisions.

16. For the purposes of this DFI, a public service agency includes departments, ministries, offices of Ministers, organisations, ventures or inter-departmental ventures, State enterprises, and Crown entities.

Authoritative version of DFI 7.2

17. The online copy of *DFI 7.2* is the authoritative version. Any printed copy or CD-ROM copy is deemed uncontrolled and is to be used for guidance only.

Related publications

A. *Cabinet Manual*

B. *Public Records Act 2005*

C. *Official Information Act 1982*

D. *Privacy Act 2020*

E. *Ombudsmen Act 1975*

F. *Harmful Digital Communications Act 2015*

G. *Harassment Act 1997*

H. *Inquiries Act 2013*

I. *Public Service Act 2020*

ANNEX A

Meanings of Terms

a. Words and phrases are to be given their ordinary grammatical or military meaning promulgated in relevant legislation, military glossaries and authorised dictionaries.

b. Meanings of terms used in this publication are—

Term	Meaning
Defence Information Environment	The Defence Information Environment consists of the data and information used by the Defence Force for its internal and external activities, and military operations, along with the means by which it is created, captured, shared, exploited, protected, stored and archived in and across all security domains.
natural person	A natural person is a person who has their own legal personality and is an individual human being.
information privacy request	A request from a person (or their representative) for their personal information that may be held by the NZDF or confirmation as to whether or not NZDF holds personal information about them.
IPP	Information Privacy Principle
near miss	An unplanned event that did not result in the disclosure of personal information, but had the potential to do so. Only a fortunate break in the chain of events prevented unauthorised disclosure of personal information.
need-to-know principle	Refers to the concept that fundamental to all aspects of privacy is that only people who receive personal information (including personal health information) are those who need it to complete their duties. Thus members of the NZDF receive access to personal information only because they 'need to know' it to complete their duties.
official information	Official information is defined in s 2(1) of the *Official Information Act 1982*. It includes any information held by the NZDF unless expressly excluded by the *Official Information Act 1982*.
OIA	*Official Information Act 1982*
PA	*Privacy Act 2000*
personal information	Information about an identifiable individual including information relating to a death that is maintained by the Registrar-General pursuant to the *Births, Deaths, Marriages, and Relationships Registration Act 1995*, or any former Act. 'Information' is not defined in the *Privacy Act 2020*, so a common sense meaning of the word applies. The information does not have to be subject to a special handling marking (eg STAFF-IN-CONFIDENCE or MEDICAL-IN-CONFIDENCE) to qualify as personal information.
PRA	*Public Records Act 2005*
publicly available personal information	Information that is in a publicly available form such as email, the internet, social media, meetings and conversations.
publicly available publication	A magazine, book, newspaper or other publication that is or will be generally available to members of the public, and includes a public register.

Term	Meaning
public interest	Public interest refers to the concept of public good (in contrast to the selfish interest of a person, group or company) in society. Public interest does not mean the whole population has to be affected. The private interests of individuals can also reflect wider public interests. Even though a requester may gain personally from receiving the information, there may still be a wider public interest to be served by its release.[3]
public-interest immunity	Public-interest immunity, previously known as 'Crown privilege', is a principle allowing one party to refrain from disclosing evidence to another party where disclosure would be damaging to the public interest.[4]
social media	Online services that enable people to stay in touch, create and share content, and participate in a range of social activities online. These include, but are not limited to, Facebook, Twitter, Instagram, LinkedIn and YouTube).
unauthorised disclosure of personal information	The unauthorised release of personal information which compromises a person's right to privacy.
well-being providers	Service providers, commanders and managers responsible for the care of NZDF personnel.

[3] For more discussion on this issue, refer to the Ombudsman's opinions at *www.ombudsman.parliament.nz*.
[4] See ss 69 and 70 of the *Evidence Act 2006*. Public interest immunity may be claimed by the Crown in situations where disclosure would be damaging to the public interest. It can be subject to judicial scrutiny and the justification for the claim must be considered on a case-by-case basis. Advice should be sought from the Crown Law Office if the NZDF wishes to claim public interest immunity from disclosure.

Part 1 - OFFICIAL INFORMATION

Chapter 1 - Legislation

1.1.1 General statement

The government holds a large quantity of all kinds of information. The law governing the creation, collection, storage, use and destruction of this information is set out mainly in the *Public Records Act 2005* (PRA) [5] and the *Privacy Act 2020* (PA). These Acts, together with the *Official Information Act 1982* (OIA), also govern the availability of this information and promote accountability of government, public service agencies and officials through transparency and reliable record-keeping. They help to ensure that information generated or obtained or held by the government is used for lawful purposes.

Section 1 - Public Records Act 2005

1.1.2 Purpose of the Public Records Act 2005

a. The purposes of the PRA include—[6]

   (1) enhancing public confidence in the integrity of official information and public records;

   (2) ensuring that full and accurate records of the affairs of central and local government are created and maintained; and

   (3) providing for the preservation of, and public access to, records of long-term value.

b. Organisations covered by the PRA are to—

   (1) create and maintain records;[7]

   (2) dispose of public records only as authorised by the Chief Archivist, or otherwise by law;[8]

   (3) transfer archival records to Archives New Zealand;[9] and

   (4) classify the access status of records.[10]

c. The PRA requires that the New Zealand Defence Force (NZDF) create and maintain records of its military and business activities, including any contracted out to third parties. This means that all records must be saved, managed and archived in accordance with the PRA.

[5] The PRA replaced the *Archives Act 1957* on 20 April 2005.
[6] See s 3 of the PRA for a complete list of the purposes of the PRA.
[7] PRA, s 17.
[8] PRA, s 18.
[9] PRA, s 21.
[10] PRA, s 43.

d. Archives New Zealand issues general disposal authorities with regulatory information that specifies types of information and records to be kept, their retention periods and their means of disposal.[11]

e. The Chief Joint Defence Services is responsible for ensuring that records management throughout the NZDF complies with the PRA and any regulations and direction made under the PRA.

f. Records include documents and information created or received by members of the NZDF in the course of their service in the Armed Forces or employment in the NZDF and that from consultants and contractors engaged for NZDF purposes. For the NZDF, this information can include, but is not limited to—

(1) emails;

(2) minutes and submissions;

(3) letters and notebooks/notes kept by members of the NZDF;

(4) orders, directives and instructions (eg direction to the NZDF promulgated in authorised publications, and other duly authorised documents giving direction and instructions to members of the NZDF and other persons employed by the NZDF);

(5) strategic and corporate planning, and policy documents and corporate publications (eg annual plans, organisational reports and risk management);

(6) policy briefings;

(7) operational documentation (eg operation orders, instructions, and post-activity reports);

(8) all briefings and correspondence in whatever form sent to ministers and staff in the ministers' offices;

(9) meeting minutes;

(10) informational documentation (eg publicity material such as brochures, magazines, press statements);

(11) radio spectrum traffic recordings and digital simulator recordings;

(12) visual and photographic material, including material stored digitally, whether on an NZDF or personal device; and

(13) all information posted on the NZDF intranet, social media and web pages.

g. The PRA also provides for the safekeeping of private records (eg personal records of service and employment history). All records must be full and accurate, and maintained in the Defence information environment, or in paper form retained in secure storage, so they remain reliable and accessible over time.

[11] For example, *General Disposal Authorities 6 and 7*.

1.1.3 Authorised disposal

a. Records disposal refers to the process of determining the fate of a record. Under the PRA, there are a number of disposal options, the most common being either to destroy or transfer as archives.

b. All disposals must be in accordance with the NZDF general disposal authorities as issued by the Chief Archivist under the PRA.

Section 2 - Official Information Act 1982

1.1.4 Purpose of the Official Information Act 1982

a. The OIA is New Zealand law that replaced the *Official Secrets Act 1951*. Whereas the *Official Secrets Act 1951* obliged Government agencies to protect information unless there was a good reason to release, the guiding principle of the OIA is that information should be made available unless a good reason exists for withholding it.

b. The purposes of the OIA[12] are defined as—

(1) progressively increasing the availability of official information to the people of New Zealand;

(2) enabling more effective participation in the making and administration of laws and policies;

(3) promoting accountability of ministers of the Crown and officials;

(4) providing proper access by an individual person to official information relating to them;

(5) enhancing respect for the law and to promote the good government of New Zealand; and

(6) protecting official information to the extent consistent with the public interest and the preservation of personal privacy.

1.1.5 Principle of availability of official information

a. The OIA allows an eligible person or persons to request and receive (unless there is a good reason to withhold) information held by ministers, government officials, and public service agencies.

b. The OIA also permits public service agencies to withhold access to, or refuse a request for, official information in certain circumstances.[13]

c. When a public service agency refuses to grant access to official information, the OIA provides that, where a judgement not to release information is made because of harmful consequences, those consequences may be overshadowed by the public interest in making the information available.[14]

[12] OIA, s 4.
[13] OIA, ss 6, 9 and 18.
[14] OIA, s 9(1).

1.1.6 Directory of Official Information

a. The Ministry of Justice promulgates a publication to assist members of the public effectively exercise their rights under the provisions of the OIA.[15] The *Directory of Official Information* assists people in two ways—

(1) it gives a detailed picture of the structure of central government departments and public service agencies, including the NZDF; and

(2) it enables people to find out where their requests for information should be made.

b. The contents of the Directory includes a description of all public service agencies covered by the OIA; their functions, structure, records, manuals, committees and contact officials.

c. The Directory of Official Information is not the authoritative list of official information held by the NZDF and any omission of information in the Directory does not (on its own) mean that the information may be withheld. Equally, just because the information is listed, it does not necessarily mean that it can be released.

1.1.7 Access to official information

NZDF policy and procedures regarding access to official information are administered and controlled by the Chief of Staff (CoS) Headquarters New Zealand Defence Force (HQNZDF). The procedures for administering the provisions of the OIA are prescribed in Part Two of this publication.

Section 3 - Privacy Act 2020

1.1.8 Purpose of the Privacy Act 2020

a. The PA controls how organisations collect, use, disclose, correct, store and provide access to personal information.

b. The PA comprises principles that reflect internationally accepted standards for the good management of personal information. These principles cover—

(1) the collection of personal information;

(2) the storage and security of personal information;

(3) requests for access to and correction of personal information;

(4) the accuracy of personal information;

(5) the use and disclosure of personal information; and

(6) using unique identifiers.

[15] OIA, s 20.

c. The purpose of the PA is to promote and protect individual privacy by[16]—

(1) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account; and

(2) giving effect to internationally-recognised privacy obligations and standards in relation to the privacy of personal information, including the Organisation for Economic Co-operation and Development (OECD) Guidelines and the International Covenant on Civil and Political Rights.

1.1.9 Administration of the Privacy Act 2020

a. The NZDF policies and procedures that implement the provisions of the PA are directed by CoS HQNZDF. The procedures for administering the provisions of the PA are prescribed in Part Three of this publication.

[16] PA, s 3.

Part 2 - NZDF POLICY FOR MANAGING OFFICIAL INFORMATION

Chapter 1 - Implementing the Official Information Act 1982

2.1.1 General application of the Official Information Act 1982

Contemporary guidance and advice on applying the provisions of the *Official Information Act 1982* (OIA) can be found on the *Ombudsman's website*.[17] The Office of the Ombudsman is also available to advise organisations and individuals on the application of the OIA.

2.1.2 NZDF policies and procedures

All requests for access to official information and general enquiries from the media and the public must be handled in accordance with the provisions of the OIA (and the *Privacy Act 2020* (PA) where applicable) and with the instructions prescribed in this publication.

2.1.3 Protective security of official information

a. Information security within the New Zealand government requires that official information must be protected by limiting access to that information through a series of measures that include—

   (1) processes that control the handling, transmission and access limitations;

   (2) physical means of protecting information (eg storage and access to work areas); and

   (3) technical protection through the use of encryption.

b. The New Zealand Government security classification system is implemented in the New Zealand Defence Force (NZDF). This requires that official information demanding extra protection against unauthorised or accidental disclosure be appropriately marked and stored with access limited to suitably cleared persons with a need to know.

c. Security classification and special handling markings are to be used to identify the security classification and special handling requirements of documents and publications. These protective markings must be used in accordance with the directions promulgated in *DFO 51 Defence Force Security Orders Vol 1*.

2.1.4 Release of official information

a. Release of official information held by the NZDF must comply with the OIA, the PA and these instructions.

[17] Eg *Agency Assistance* and *The Ombudsmen Quarterly Review.*

b. NZDF publications (Defence Force Orders, Defence Force Instructions and Defence Force Manuals) may be released to the public in certain circumstances. The release of NZDF publications falls into two categories and must be stated on the cover of the publication accordingly—

(1) ***Releasable to the public***. There are no limitations, protective security caveats or special handling markings preventing the release of the document to persons external to the NZDF.

(2) ***Not releasable to the public***. The content is of special use by members of the NZDF. The publication is protected by security classification, special handling provisions or is solely for use by members of the NZDF or approved persons engaged for NZDF purposes.[18]

c. Where there is any doubt concerning the suitability for release of official information, due to its security classification, special handling caveats or sensitivity, the request must be referred to the Chief of Staff (CoS) Headquarters New Zealand Defence Force (HQNZDF).

d. When approved for release, all documentation and NZDF publications released on request, under the provisions of the OIA or the PA, must be marked in accordance with the instructions promulgated in this *DFI 7.2 Official Information*.

2.1.5 Copyright

Publications and documentation authored or written by members of the NZDF or by contractors and consultants engaged for NZDF purposes are the property of the NZDF. The text of publications and documents may be reproduced for use by members of the NZDF. The reproduction of any text for other purposes without approval is prohibited. NZDF publications must have the following notice applied on the front cover of publications—

> *©Crown Copyright [year of publication]. This document is the property of the New Zealand Defence Force. The text in this document may be reproduced for use by members of the New Zealand Defence Force. Crown Copyright material must not be used or reproduced for any other purpose without prior permission of the Chief of Defence Force.*

[18] All or part of these documents may be re-classified or redacted for release in consultation with the originator.

Chapter 2 - General Principles of the Official Information Act 1982

2.2.1 Defining official information

a. Official information is defined in s 2 of the *Official Information Act 1982* (OIA). In accordance with the OIA, official information means any information held by the New Zealand Defence Force (NZDF). Official information can include—

(1) electronic mail (held on NZDF and personal devices);

(2) text messages (transmitted and received on NZDF and personal devices);

(3) minutes and submissions;

(4) letters;

(5) orders, directives and instructions (eg direction to the NZDF promulgated in authorised NZDF publications, directives and administrative instructions);

(6) all information recorded or archived in the Defence digital information environment;

(7) policy briefings;

(8) operational documentation (eg operation orders, instructions, and post-activity reports including 'lessons learned');

(9) maps, plans, graphs, drawings, notes and notebooks;

(10) all briefings and correspondence in any form sent to ministers and staff in the ministers' offices;

(11) draft documents and oral conversations (including taped records);

(12) knowledge or information held or known by members of the NZDF, but not written down;

(13) meeting agenda and meeting minutes;

(14) documentation created by a third party and held by the NZDF;

(15) informational documentation (eg publicity material such as brochures, magazines, press statements);

(16) visual and photographic media;

(17) radio spectrum traffic recordings and digital simulator recordings;

(18) web pages on the internal and external-facing websites; and

(19) information amassed in personnel files and employee records.

b. Personal information means information about an identifiable individual and includes information relating to a deceased person.[19] Information privacy principle six of the PA allows for individuals to request confirmation of the existence of information held on

[19] This is the definition from the *Privacy Act 2020* (PA); s 2 of the OIA defines personal information as "any official information held about an identifiable person".

them and have access to that information. The NZDF procedures for handling requests for personal information are detailed in Part Three of this publication.

c. Information generated by consultants or contractors for the NZDF, including drafts and working copies, is deemed to be official information held by the NZDF.

d. In accordance with the OIA,[20] official information is not, eg—

(1) evidence given or submissions made to a Court of Inquiry, a Royal Commission or other inquiry convened under the *Inquiries Act 2013*, or information subject to an order issued under s 15 of the *Inquiries Act 2013*;

(2) information held by the NZDF or a Minister of the Crown as an agent for the sole purpose of safe custody;

(3) information contained in any correspondence or communication that has taken place between the NZDF and the office of the Ombudsmen and relates to an Ombudsman investigation (other than information that came into existence before the commencement of that investigation); or

(4) information contained in any correspondence or communication that has taken place between the NZDF and the office of the Privacy Commissioner and relates to a Privacy Commissioner investigation (other than information that came into existence before the commencement of that investigation).

2.2.2 Right of access to official information

a. Eligibility[21] to access official information held by the NZDF is—

(1) any person being—

(a) a New Zealand citizen;

(b) a permanent resident of New Zealand;

(c) a person who is in New Zealand;

(d) a body corporate that is incorporated in New Zealand; or

(e) a body corporate that is incorporated outside New Zealand but that has a place of business in New Zealand.

b. Persons making a request for access to personal information may be asked to provide proof of identity when seeking information about themselves.[22]

c. Persons making an official information request do not need to give reasons for requesting official information.

[20] Refer to the OIA for the full list of exclusions.
[21] OIA, s 12 (Ombudsman's guidance on s 12 indicates that the principle of availability outweighs any reason to decline a request if the person does not meet s 12 criteria).
[22] OIA, s 25(a).

d. A person asking that their request be treated as urgent must give their reasons for seeking the information urgently. On receiving an urgent request, the NZDF must consider the request and the reason stated for its urgency when determining the priority to be given to responding to it.[23]

2.2.3 Requests for access to official information

a. A request for access to official information may be made verbally or in writing directly to the Minister of Defence, the Minister for Veterans, or members of the NZDF, including Defence Public Affairs.

b. A request for access to official information held by the NZDF may be made in any form and communicated by any means. It may be made in writing, verbally, posted to the NZDF website or other web-based application, email, phone or in conversation.

c. It is preferable that a request be made in writing. If the request is made verbally, it is helpful if the request is followed up with a written confirmation at the earliest opportunity to ensure that the exact information can be provided.

d. If a requester declines to put a verbal request in writing, the person receiving the request must record their understanding of the request and provide a copy to the requester.

e. A request for access to official information does not need to specifically refer to the provisions of the OIA in the request to be a request under the OIA.

f. A request should be presented with clarity and exactitude of the information being sought. If it is not then the requester should be asked to refine or otherwise make clear what information is sought.

g. The Chief of Staff (CoS) Headquarters New Zealand Defence Force (HQNZDF) and members of the NZDF authorised to respond to official information requests must provide every assistance to a person requesting access to official information even when a request may not have been presented in a recognised manner.

2.2.4 Withholding the release of official information

a. Official information must be made available unless there is a good reason to withhold it.[24] The OIA sets out a number of reasons for which information may be withheld. These reasons, among others, include —

(1) prejudice to the security and defence of New Zealand or the international relations of the Government;

(2) prejudice to the maintenance of the law;

(3) prejudice to legal professional privilege;

(4) preservation of privacy; and

(5) protection of information that has been received in confidence.[25]

[23] OIA, s 41(3).
[24] OIA, s 18.
[25] OIA, ss 6 and 9.

b. Where a document includes information that may be withheld under the provisions of the OIA, that document may be released with the information deleted (or redacted) as necessary.[26]

[26] OIA, s 17. Alternatively a summary of the information may be released under s 16 of the OIA.

Chapter 3 - Role of the Chief Ombudsman

2.3.1 Chief Ombudsman

a. For the purpose of the *Official Information Act 1982* (OIA), the role of the Chief Ombudsman and the Ombudsman's Office is to—

(1) investigate OIA-related complaints referred to the Ombudsman's Office; and

(2) investigate, monitor and report on the official information-related activities of agencies that apply the OIA.

b. The Ombudsman may investigate or review any decision made by a Minister of the Crown or public service agency that[27]—

(1) refuses to make official information available to an eligible person;

(2) imposes conditions on the use, communication, or publication of the official information requested;

(3) has not responded to the request in a reasonable timeframe (noting that the 20 working day time limit set out in the OIA may be extended for various reasons); or

(4) has not, in the view of the requester, made a document available or provided access to official information in an acceptable format or where a charge has been applied or requested for the information.

c. The Ombudsman routinely reviews government agencies' compliance of the OIA. The Ombudsman's Office also publishes data on the results of complaints they receive every six months. These reports are made public on the *Ombudsman's website*.

[27] OIA, s 28.

Chapter 4 - Contact with the Media and Communicating in Public

2.4.1 Communicating official information to the public

a. These instructions set out the rules that all members of the New Zealand Defence Force (NZDF) must follow if they wish to have contact with the media, or write or speak publicly on NZDF or governmental matters.[28] For the avoidance of doubt, these instructions apply equally to—

(1) all members of the NZDF;

(2) locally employed civilians engaged to work overseas under s 90A of the *Defence Act 1990*;

(3) all persons from foreign military forces on loan or secondment, or otherwise working under the administrative control of the NZDF or one of the Service arms;

(4) employees of governmental agencies who, on occasion, are seconded to the NZDF;

(5) independent contractors (including consultants) engaged by the NZDF; and

(6) members of the New Zealand Cadet Forces (NZCF).

b. These instructions do not apply to elected officials of a recognised employment union or staff association when they publicise the association's or union's views on a particular matter because it directly affects the employment of the civil staff.

c. These instructions are put in place to make sure that operational and personal security is maintained and standards of political impartiality and public accountability are met at all times.

d. Examples of communicating with the public include—

(1) publishing material or submitting material with the intention or likelihood of publication in any medium outside the NZDF;

(2) self-publishing or releasing material on the Internet, including through social media, messaging applications or online sharing applications;

(3) speeches and presentations where the media or public may be present;

(4) completing external questionnaires, engaging in surveys, polls or contributing to research projects where an individual's role or experience in the NZDF is a key prerequisite for participation;

(5) contributing any Defence-related material to an online community or shared electronic information resource (eg bulletin boards or newsgroups) apart from in a personal capacity; and

(6) when requested to provide comment for a supplier or potential supplier concerning the provision of goods and services to the NZDF.

[28] 'Contact' in this context means passing information or expressing opinions on matters relating to Defence.

e. Within prescribed security constraints, the NZDF maintains a policy of openness about its activities. It is important that members of the NZDF are able to, for the most part, explain their roles and government policies and decisions relating to the defence of New Zealand. However, such contact must be properly authorised to ensure that it is appropriate, worthwhile and protects members of the NZDF against possible misreporting.

f. While observing the need for security and the confidentiality of many NZDF activities, members of the NZDF have a responsibility for maintaining good relations with the public and the media. Media includes not only newspapers and periodicals but also other publications, radio, television, films, video, social media, the internet and all other means of communicating official information.

g. All members of the NZDF and others to whom these instructions apply must exercise honesty and not undertake any activity that may call into question their political impartiality, Service reputation or the reputation of the NZDF generally when communicating official information to the public.

h. In all cases, the impact of any communication must be considered carefully, both in terms of the effect on the intended audience and on any unintended audience through subsequent coverage by the media. It is the responsibility of all personnel to minimise the scope for misreporting and misrepresentation and not stray beyond the issues on which they have been approved to speak.

i. At any time, a media representative or other person who seeks information on a Defence-related matter from a member of the NZDF (who is not authorised to speak on the matter) is to be invited to contact Defence Public Affairs or submit a request for access to official information in accordance with the *Official Information Act 1982* (OIA).

2.4.2 Communicating in public

a. There are inherent risks that come with communicating in public. All members of the NZDF—

   (1) have an overriding obligation to protect operational and personal security;

   (2) must comply with the law and all NZDF protective security orders and instructions;

   (3) have an obligation to protect the organisation's intellectual property rights.

b. These instructions cover—

   (1) engagement with the media;

   (2) the publication of material either in print or online (eg books, articles, academic papers, audio, still imagery, video or other content), in any medium available outside of the NZDF;

   (3) speeches and presentations at conferences or other events where the public or media may be present;

(4) communicating online and through social media (eg Facebook, Twitter, Instagram); and

(5) all other forms of public engagement.

c. Before considering contact with news media or communicating in public, the following factors must be considered—

(1) Is there a risk to operational security, or of disclosure of sensitive information or information protected under either governmental Protective Security Requirements or NZDF policies?

(2) Could the NZDF or Service reputation be compromised?

(3) Are there international relations implications?

(4) Would this call into question either the NZDF or the individual's political impartiality?

(5) Are there commercial implications, including ensuring that neither the NZDF nor the individual endorses or appears to endorse any particular company, product or service?

(6) Are there any relevant legal implications? For example, it may be that matters cannot be spoken of because they are before the courts, protected by orders made by the courts, under the *Inquiries Act 2013* or protected because they relate to the terms of confidential settlements, etc.

d. The Chief Adviser Public Affairs (Office of the Chief of Defence Force [OCDF]) is the principal adviser on communicating with media representatives and organisations. This role is exercised with, and alongside, Defence Public Affairs (DPA).

e. The Chief Adviser Public Affairs, in consultation with the Chief of Staff (CoS) Headquarters New Zealand Defence Force (HQNZDF) and Chief of Defence Force (CDF), is responsible for managing external communication to the media and the public.

f. Chiefs of Service (COS), in concert with DPA, are responsible for managing any Servicepersons' presentation of written material in the form of memoirs, biographies, professional commentaries and similar journals. Prior to any publication, the nature of this work and any related issues are to be advised to the OCDF.

2.4.3 Communication means and processes

a. **Contact with the news media**. The Director Defence Public Affairs, to whom the media team report, is responsible for managing contact with news media including both proactive and reactive media handling. The Director Defence Public Affairs (D DPA) will consult with stakeholders when drafting a response. The Chief Adviser Public Affairs will judge whether ministers need to be informed before engagement with the news media takes place.

(1) Contact activities include—

(a) contact with journalists, reporters and similar persons;

(b) contact with individuals with known links to the media through commentators in academia, industry, think-tanks or lobbyists;

(c) contributing to online debates or commenting on online issues;

(d) participating in radio or television programmes and phone-ins on any topic related to Defence matters;

(e) contact with media when attending external events such as conferences or seminars;

(f) issuing invitations to media representatives for press briefings and NZDF events.

(2) COS, Commander Joint Forces, formation commanders and Base/Camp commanders may speak to regional or local media on routine matters specifically related to their own area of responsibility. They may comment on other government or defence issues as a spokesperson by arrangement with DPA. A record must be kept of the contact and DPA media team informed.

(3) The Commander Joint Forces, in consultation with the Chief Adviser Public Affairs and Defence Public Affairs, may authorise contact with foreign media in operational theatres.

(4) Resident Defence Attachés/Advisers (DAs) may engage with the host nation's national or local media subject to any instructions that the resident New Zealand High Commissioner or Ambassador may issue to accredited Defence Staff.

(5) Any member of the NZDF who is approached by a journalist or a third party with known links to the news media (including former members of the NZDF) on any Defence matter should refer the matter to the DPA media team as soon as possible, unless they are specifically authorised to speak on that matter. This includes approaches made in a social setting whether the event is work related or not.

(6) Members of the NZDF may, in their official capacity, relay information on a Defence or Government matter when authorised to do so. Permission should be sought in advance when speaking or engaging on sensitive, or potentially sensitive issues.

b. **Speaking in public**. Public speaking at conferences, events, lectures and in the community offer opportunities for members of the NZDF to engage with important audiences. Careful consideration must be given to the value of speaking in public and any associated risks. Where a number of NZDF persons are asked to speak at a particular event, notification, central coordination and assistance is to be sought from Defence Public Affairs.

c. **Communicating online and through social media**. The NZDF recognises social media and other online tools can be an important means for members of the NZDF to keep in touch with family, friends and colleagues, as well as professional communities of interest. The NZDF encourages the proper use of these tools where safe and appropriate. When using these means of communication, which includes the posting of images, audio, videos and writing, all personnel must—

(1) follow the same high standards of conduct and behaviour online as would be expected elsewhere;

(2) always protect personal information and operational security;

(3) get command authorisation when appropriate; and

(4) ensure that the reputation of the Armed Forces, and NZDF as a whole is not compromised.

d. Personnel do not need to seek permission when communicating online about non-Defence matters; but they must do so before communicating about Defence matters as outlined in paragraph *2.4.2*. This applies regardless of whether an individual posts online in their own name or under a pseudonym; any such pseudonym must be declared when seeking approval.

e. Instructions for the NZDF use of social media are in *Annex 2-A*.

f. The Director of Defence Security (DDS) publishes guidelines for the proper and safe use of social media.[29]

g. **Media channels**. The D DPA is accountable for ensuring that arrangements are in place for handling specific media channels (other than news). These projects typically refer to magazines, books, television and radio programmes, documentaries and reports of NZDF projects.

h. **NZDF in-house publications**. Editors and those persons contributing content to approved internal publications with an external readership (eg Service periodicals or those publications made available on the Internet) must ensure that no sensitive or obviously contentious material is inadvertently released.

i. **Contact with Members of Parliament (MPs).** All contact between any members of the NZDF, and MPs and their staff in an official capacity must be authorised in advance by the CoS HQNZDF.

(1) This rule does not apply to members of the NZDF contacting their constituency MP on matters that concern them personally. Under no circumstances are matters related to an NZDF member's work to be communicated with a constituency MP outside of professional Defence and/or Parliamentary processes.

(2) Any invitation to speak to MPs, including all-party parliamentary groups, must be treated in the same way as any other public communication. An invitation to speak to MPs cannot be accepted until endorsed by the Minister of Defence. Individuals must then present the proposed speaking material to the Chief Adviser Public Affairs and seek formal approval.[30]

j. **Request for comment from suppliers**. The NZDF policy in respect of suppliers is that, as an impartial public service agency, members of the NZDF may only make brief factual statements in respect of contractual positions unless contractual obligations and/or other commercial sensitivities prohibit such comment.

[29] *Social Media Handbook*.
[30] Includes speech notes and any visual material to be used during the presentation.

(1) Members of the NZDF must not express a preference for, or give the perception of an endorsement of any company, product or service. Any request from suppliers for input to their press releases or public relations material (eg annual reports or newsletters) must be approved by the Chief Joint Defence Services in consultation with the Chief Adviser Public Affairs.

(2) The authority to use the NZDF identity by third parties resides only with CDF.[31] Members of the NZDF have no delegated authority to permit third parties to use any badge, logo, insignia or device that comprises any elements of the NZDF identity.

2.4.4 Security considerations

a. **Operational security**. All members of the NZDF must protect operational security, avoid actions that might damage relations with other nations, or harm the security or other interests of security partners. Personnel must not pass on any classified or other information that has not been authorised for release, including to family and friends. Persons wishing to speak or write about their operational experiences must consult with their COS and DPA, and may seek the advice of the Chief Adviser Public Affairs.

b. **Personal security**. There are inherent risks in communicating in public, which have been heightened by the growing use of online communications. Social media in particular can present risks to operational and personal security unless users take appropriate steps to safeguard their information. Unsafe use of these communications, most likely through deliberate or inadvertent posting of private information or details, can compromise both personal and operational safety. The risk is highest when mass information in the public domain can be used to link Service information with personal details, which could be used to target members of the NZDF community. Once online, this information is often permanently available and easily replicated on other media channels.

c. **Other considerations.** Personnel must remain aware at all times that anything they say or write in public may be reported and publicised. Commercially sensitive material must not be disclosed without good reason under the OIA, and the NZDF and security partners' intellectual property rights must be protected.

2.4.5 Monitoring social media communication channels

a. The NZDF uses keywords to monitor online activity that references the NZDF and its activities. Where appropriate, this may result in the review of the content of personal accounts should an inappropriate post be published by a member of the NZDF.

b. The NZDF moderates authorised accounts and reserves the right to remove any post or comment that does not comply with the terms and conditions of use for a particular social media platform used by the NZDF. The NZDF will occasionally remove content that—

(1) is not relevant;

[31] NZDF Visual Identity Guidelines 2018.

(2) breaches legislation, copyright or intellectual property rights;

(3) is offensive or discriminatory;

(4) demonstrates political bias or is otherwise political in nature;

(5) relates to commercial activity, including advertising;

(6) contains profane, offensive, inappropriate, threatening or discriminatory language;

(7) posts personal information, including photos or video, of persons without their consent;

(8) is considered 'spam' (the same or similar content posted repeatedly);

(9) is considered disruptive or can be considered 'trolling' (content that is inflammatory or off-topic and designed to create discord and controversy);

(10) link-baits (embedded links in a post that draws others to another site); or

(11) does not comply with generally accepted conduct or social behaviour.

c. Any person who has concerns about the content of official media accounts should advise the D DPA without delay.

d. The D DPA is responsible for monitoring the reputation of the NZDF online through clear, consistent and accurate messaging, for reviewing any incidents brought to their attention and for reporting any violations regarding the use of social media to the Chief Adviser Public Affairs.

Annex to Chapter 4

2-A Instructions for the Use of Social Media

ANNEX 2-A

INSTRUCTIONS FOR THE USE OF SOCIAL MEDIA[32]

Social media

1. Social media is a set of online interactive technologies, sites and practices that are used to share opinions, experiences and perspectives. The use of this means of engaging with the community must be considered alongside the traditional media and carefully managed.

2. The main benefit of social media for the NZDF is that a well-considered and carefully implemented social media plan can create greater transparency, an interactive relationship with the public, a means of demonstrating the professionalism and values of the NZDF and engender more public trust in the organisation.

3. While social media consists of personal views and interactions online, mainstream media constantly scrutinise most forms of social media, and stories can result from that monitoring. Social media can require quick responses and direct communication with interested parties, often in real or near-real time. Information posted on social media by members of the NZDF in their official capacity must be accurate and verifiable, and any contentious issues must be escalated to higher authority as soon as they are identified.

4. Members of the NZDF may use social media as either a representative of the NZDF making official comment or in their private capacity in accordance with this instruction.

Use of social media for official purposes

5. The protocols that apply when acting as an official representative of the NZDF are the same whether communicating with the media, speaking at a conference or using social media. All members of the NZDF should only disclose information, make commitments or engage in activities when authorised to do so. Comments will often be permanently available and able to be reproduced in other media.

6. The use of social media for official NZDF purposes must—

   a. provide the public with balanced and objective information to assist them understand the role and professionalism of the NZDF; and

   b. keep the public informed of issues of significant interest to the wider community.

7. The use of social media for communicating with the public must be appropriate. Any member of the NZDF authorised to administer an NZDF social media site must be knowledgeable and adequately trained in using social media before they start. Content posted in error on social media often cannot be withdrawn and may damage the NZDF's reputation and the professional reputation of the command.

8. The use of social media as a means of communication must not replace or undermine NZDF media and public affairs commentary approved by the D DPA. Any activity that represents NZDF on social media must be considered fully covered by the OIA and the obligations and representations established therein.

[32] To be read in conjunction with the NZDF Social Media Handbook.

9. The D DPA is accountable to CDF, through the CoS, for the proper and appropriate use of all NZDF media and the operation of official social media applications as prescribed below.

10. The D DPA must approve the creation and operation of official social media accounts, pages, groups or similar applications for the purposes of conveying official information or, likewise, other information that is connected with NZDF activities.

11. Within the NZDF, there are three categories of social media means of communicating information to the public. These accounts are all subject to the provisions of the OIA.

    a. **NZDF corporate social media accounts.** These are approved accounts operated by authorised NZDF persons under the direct control of the D DPA and used for communicating official information to the public.

    b. **Approved NZDF social media accounts.** These are accounts approved by the D DPA, operated in accordance with these instructions and any updated guidance issued by the D DPA. Operation of the account is to be by authorised NZDF persons under the control of the owner of the account and may be used for communicating information of a general nature to members of the NZDF and other persons.

    c. **Personal accounts used to represent the NZDF in an official capacity.** These accounts are generally operated by a member of the NZDF to maintain connectivity with their community of interest. Posts made by personnel to these accounts represent NZDF or an NZDF role in an official capacity.

12. Persons authorised to operate an NZDF official social media account must check their account regularly and respond to any request for information that may be posted on the site in a manner consistent with the NZDF's obligations under the OIA.

13. Social media accounts may also be set up by former Servicepersons or employees for the express purpose of maintaining contact with former colleagues. These accounts are considered personal and not subject to the provisions of the OIA.

14. These instructions apply no matter whether the engagement on social media sites takes place while members of the NZDF are travelling on official duty, representing the NZDF or while working from home.

15. The D DPA is responsible for the provision of awareness, specialist advice and guidance as applicable to members of the NZDF in the use of social media for official purposes.

16. A number of legal issues can arise in the deployment of social media. Legal advice should be sought to determine whether there is legal risk and what can be done to mitigate and/or respond to it.

17. The use of social media by members of the NZDF for official purposes must not communicate information that—

    a. is inaccurate or unverifiable (including the retransmission of other content);

    b. is classified, sensitive or has security implications;

c. is potentially contentious (advice should be sought from the D DPA, Chief Advisor Public Affairs and/or CoS HQNZDF to define whether an issue is contentious or not);

d. is legally privileged;

e. may impact on the safety or security of NZDF personnel;

f. may be perceived to make comment on political matters;

g. may have privacy issues;

h. is defamatory or has objectionable content;

i. has commercial content in the message;

j. breaches any applicable legislation; or

k. may have issues arising from intellectual property rights.

18. Social media presents risks. Risks need to be recognised and managed before engaging in the use of social media. All social media awareness and education activities and resources programmes must ensure that managing risks is a mandatory discussion element of a syllabus.

19. A member of the NZDF who communicates on social media for official purposes is individually responsible and accountable for their actions and appropriate use of the social media. The NZDF must be prepared to manage the potential for the improper use of social media by members of the NZDF. Improper communications on a social media site by a member of the NZDF may have disciplinary consequences or result in sanctions.

20. Most social media sites require users to accept terms and conditions under which they are required to indemnify the site owner against improper use of their site. However, there are limited circumstances under which public service agencies can provide indemnities. Therefore, before accepting the terms and conditions of any social media sites intended to be used for official purposes, members of the NZDF must seek advice from Defence Legal Services.

Responsible use of social media in a private capacity

21. Members of the Armed Forces and Civil Staff have the right to freedom of expression[33] but this right may be subject to reasonable limits prescribed by law.[34]

Caution. In advice provided to the NZDF on 3 July 2017, the Chief Ombudsman found that any information, video or photo captured or transmitted on an official NZDF or personal device that has been obtained while a member of the NZDF is acting in their official capacity is official information and subject to the provisions of the OIA.

22. Members of the NZDF who engage via social media and post content that reflects seriously and adversely on the NZDF may be subject to disciplinary proceedings under the *Armed Forces Discipline Act 1971* or the provisions of the Civil Staff Code of Conduct. This includes, but is not limited to, posts that adversely impact on the public's

[33] *New Zealand Bill of Rights Act 1990*, s 14.
[34] *New Zealand Bill of Rights Act 1990*, s 5.

confidence in the ability of an individual to carry out their official duties impartially and effectively, or that significantly impact on their working relationships.

23. Members of the NZDF may make personal use of NZDF devices and ICT facilities, or use their own personal devices to engage on social media during normal work hours provided that their use is appropriate, limited, reasonable and does not affect their work productivity.

24. Regardless of the social media being used, the owner of any personal social media account must not disclose any NZDF information that is not available to the public unless specifically authorised.

25. When choosing to use social media in a personal capacity, members of the NZDF—

    a. must not use their workplace email address to register for, subscribe or otherwise log into social media sites;

    b. must be aware that under some social media sites' terms of service, potentially all material posted becomes public information that can be freely accessed and used by others and, more importantly, becomes the property of the networking host; generally, a person no longer has control over what, where and how that information is used;

    c. must understand that they may be identified as members of the NZDF, whether or not they explicitly refer to their Service or employment even when they respond under a pseudonym or alias;

    d. must not use the identity or likeness (including photographs) of another Serviceperson or employee without their consent;

    e. must be respectful and polite and consistent with the terms of the social media platform and observe any copyright rights; and

    f. must not give rise to an actual or perceived conflict of interest with their Service or employment in the NZDF.

Staying safe on social media

26. All members of the NZDF need to be careful about the information they share and how to protect it. Others can inadvertently or intentionally use other people's personal information to embarrass or damage their reputation, or even steal their identity. The advice below applies to NZDF official social media sites and private social media sites.

    a. **Privacy and security settings exist for a reason**. Use these settings to control who sees a post or contributes to a theme – "Once posted, always posted". What is posted almost always remains online. Before making a post, be sure that it is not information or a picture you would not want your parents, colleagues or employer to see.[35]

    b. **Keep personal information personal**. Be cautious about how much personal information is provided on social networking sites. The more information that is

[35] A 2017 CareerBuilder survey found that 70% of employers use social media to screen candidates. This same survey found that 54% of employers did not hire a candidate after finding content on social media.

publicly available, the easier it is for another person to use that information to steal your identity, access your data or commit other crimes.

c. **Strategies for managing risk around the workplace**. Strategies for managing risks on personal social media include not identifying your workplace on personal social media sites and not using GPS tracking functionality.

d. **Know and manage your friends**. Carefully consider who should be granted access to a personal social media account (eg when adding friends or giving access to photograph albums). Use the embedded tools to manage information that is shared with different groups.

e. **Be honest**. If a colleague posts a comment about a person that makes another feel uncomfortable or is inappropriate, let them know. Don't retaliate by posting an equally inappropriate comment.

f. **Consider what you post before you post it**. Take time to think before posting a comment. It is easy to post a quick response to a contentious issue, then regret it.

g. **Take action**. If a threat is received or there is an element of harassment in a post, you should immediately remove that person from your friends list, block them and report the incident to the site administrator. If a threat is serious, report the matter to the Police.

Chapter 5 - Managing Requests for Information to the NZDF

Section 1 - Compliance with the Official Information Act 1982

2.5.1 Accountability and responsibility for compliance with the Official Information Act 1982

a. The Chief of Defence Force (CDF) is the accountable decision-maker on requests for official information made specifically to the New Zealand Defence Force (NZDF). This role is exercised by the Chief of Staff (CoS) Headquarters New Zealand Defence Force (HQNZDF) on behalf of CDF.

b. The CoS HQNZDF is accountable to CDF for the organisation's practices and compliance with the *Official Information Act 1982* (OIA) and the *Privacy Act 2020* (PA), the effectiveness of the procedures and the reporting of requests for information to commanders and senior NZDF executives.

c. Specifically, the CoS HQNZDF must ensure that all parts of the NZDF are aware of NZDF policies and procedures and requirements of the OIA and the PA.

d. Chiefs of Service (COS), commanders and senior executives are responsible for ensuring that all NZDF policies and procedures as they apply to the provisions of the OIA and the PA are followed.

e. Requests for access to official information must be managed consistently across the whole of the NZDF. No part of the organisation is to adopt procedures that are not compliant with these instructions.

f. The Public Service Commission publishes data on agency compliance with the OIA every six months. This data is used to gauge the effective openness and transparency of agencies to ensure they are meeting government expectations.

Section 2 - Coordinating requests for access to official information

2.5.2 Coordination

a. The NZDF operates a partially centralised model for complying with the OIA, whereby the Corporate and Ministerial Services Team manages responses to requests for information that require the considered application of the OIA. The Corporate and Ministerial Services Team can also provide advice to members of the NZDF when they are responding to requests under the PA.

b. While a request for information may be made to any person in any part of the NZDF, the coordination of access to official information is undertaken by the Office of the Chief of Defence Force (OCDF) and the direct oversight of the CoS HQNZDF. This ensures that the coordination and processing of all requests requiring the considered application of the relevant legislation are—

(1) compliant with the OIA and PA (where relevant);

(2) prepared with the full support of subject matter experts;

(3) decision-making on the release of official information is at the appropriate level;

(4) consulted with the minister when necessary; and

(5) reported accurately.

c. Media requests for information and general enquires from the public made through the media gateway, especially those seeking a quick response, are coordinated by Defence Public Affairs (DPA), under the oversight of the Chief Advisor Public Affairs and CoS HQNZDF.

d. The NZDF has a number of social media applications that are used to communicate information about NZDF activities to the public, eg Facebook, Twitter and Instagram. These sites must be monitored regularly by the owner of the site for comments or responses that may include a request for access to official information. Any request for access to official information made by way of this media must be acknowledged as soon as practicable and within the statutory timeframe.

2.5.3 Requests for information to the Minister of Defence/Minister for Veterans

a. The ministers remain the accountable decision-makers on requests for access to official information made or transferred to the ministers and their offices, albeit they routinely allocate much of the preparation to the OCDF.

b. Enquiries to the NZDF from the ministers' offices relating to official information are administered by the OCDF. If the information requested is held by the NZDF, then the request is transferred to the NZDF for action.[36]

c. Disclosure of personal information to ministers and further disclosure of such information by ministers is addressed in Part 3 of this DFI under PA considerations.

d. If the CoS HQNZDF considers that the information held by the relevant minister should not be released, then the relevant minister's office is to be informed of the NZDF recommendation with an explanation of the reasons for such a recommendation and any supporting documentation.

2.5.4 Consultation with ministers

a. The NZDF may consult the Minister of Defence about any request for official information it receives, but the decision on how to respond to the request must be made by CDF in accordance with the OIA.

b. The 'no surprises' principle adopted by ministers is intended to assist in disciplined government, transparency of decision-making and fostering an informed public. In principle, the minister or their political advisers may be informed of any requests made under the provisions of the OIA received by the NZDF, but at no time is improper influence to be applied to the content or timing of a response to a request for official information.

[36] Section 14 of the *Official Information Act 1982*.

c. When advising ministers of requests for access to official information held by the NZDF, the minister must be made aware that the NZDF is consulting and not seeking the minister's approval to release the requested information. Seeking clearance or approval for the release of information from the minister compromises the CDF's accountability.

d. Sufficient time should be allowed for the minister's office to raise any concerns about the proposed decision.

e. On being consulted, the minister may take the view that information the NZDF wishes to release should not be released. In such a case, transferring the request to the minister may be an appropriate course of action if the requirements of the OIA can be satisfied. Nonetheless, a disagreement with respect to a response is not, on its own, a reason to transfer any request.[37]

f. Where the request is not transferred to the minister, the views of the minister are not determinative, and an assessment needs to be made by CDF as to whether any of the withholding provisions apply.

g. CDF should advise ministers if the NZDF intends to release any information that is particularly sensitive or potentially controversial. A notification of this nature is not the same as consultation and must not delay the release of information.

h. Where there is a disagreement about a response to a request by the NZDF, CDF is accountable for deciding to release official information. While advice from the minister's office may be helpful, should the CoS HQNZDF consider that the demands or matters of disagreement by ministerial/political advisers risk interfering with the CDF's statutory accountabilities and responsibilities, the matter must be referred to the CDF without delay.

i. The NZDF must seek approval from the relevant minister if the request relates to current Cabinet material that has not already been publicly released. In the case of Cabinet papers approved under a previous government, Ministerial Services will consult with the Department of the Prime Minister and Cabinet (DPMC).

j. If there is any doubt, advice on ministerial consultation or notification may be sought from the Public Services Commission or the Office of the Ombudsman.

k. More detailed instructions for managing OIA requests involving ministers are in *Annex 2-B*.

2.5.5 Providing information to select committees

a. Select committees have the right to request information from ministers and the NZDF under *Standing Order 191 of the House of Representatives*. The NZDF is expected to meet these requests unless it is not in the public interest to do so.

[37] OIA, s 14.

b. There may be valid reasons to protect the information from public release if the information requested is classified or sensitive. In these circumstances, a select committee may waive the request or consider a compromise option, such as a summary of the information.

c. The minister has the ultimate responsibility for the release of the information to a select committee and must be consulted. Members of the NZDF who may appear before select committees in support of the minister have an obligation to manage risks and apply the 'no surprises' approach when briefing the minister.

2.5.6 Requests for parliamentary information

In the normal course of its operations, the NZDF holds a wide range of material relating to parliamentary proceedings and the minister. While most documents relating to these proceedings are routinely made available to the public by the Office of the Clerk, many require the approval of the minister to release the information (eg Cabinet papers or ministers' briefing papers). Some information and proceedings remain secret as defined by *Standing Order 223 of the House of Representatives* and are treated in accordance with the provisions of that Order and the practices of the House. These documents must not be released without the advice of the Office of the Clerk.

2.5.7 Release of legal advice

a. In providing CDF with all relevant information and advice before making a decision on a particular matter, some NZDF documents will, out of necessity, include legal advice that may be protected from disclosure under 'legal professional privilege'.

b. Legal professional privilege is a term applied to the protection of confidential communications between a lawyer and a client for the purposes of giving and receiving legal advice or in connection with litigation. If legal advice is protected by legal professional privilege it may be protected from disclosure under the OIA and the PA. It is important that legal professional privilege in any legal advice offered to the minister or CDF is maintained and not unintentionally relinquished.

c. All legal advice provided to the minister or members of the NZDF (whether by Defence Legal Services (DLS), the Crown Law Office or an external lawyer) will attract legal professional privilege. A document does not automatically attract legal professional privilege merely because a lawyer prepared it or it is endorsed 'legally privileged'.

d. Some material held by the NZDF will also be protected by litigation privilege which is part of legal professional privilege.

e. The NZDF cannot disclose or publicly release legally privileged material without the consent of the Attorney-General, as the Crown is the client of all advice. To ensure that legal advice provided to members of the NZDF or the minister is properly protected by legal professional privilege, all those involved in preparing documents containing legal advice for public release must consult with DLS before making decisions on such documents.

2.5.8 Release of names and contact details

a. The name, position and work contact details of members of the NZDF should be released if all it reveals is their official role.

b. There are special reasons to withhold or redact names, positions and/or contact details in specific circumstances, such as—

(1) when release of their name or position would prejudice the security or defence of New Zealand;

(2) for the protection of personal safety (eg when personnel are deployed in situations where release of their names could endanger their safety);

(3) when in the course of their duties, there is a reasonable expectation that the release of names could expose members of the NZDF to improper pressure or harassment and have the potential for an adverse impact on the people concerned and NZDF activities;

(4) when release of the name or contact details would reveal something private or personal about them; or

(5) to mitigate the adverse effect that connection to opinion material can have on providing further opinions that are necessary for the proper conduct of public affairs.

c. Other reasons to withhold or redact names under the OIA may exist and, therefore, consultation with Corporate and Ministerial Services is required where doubt exists as to whether information should be withheld or redacted.

d. In general, when personal information forms part of an email signature block routinely sent to external recipients, or where these details can be inferred, the withholding or redaction of personal details should not occur (unless reasons for withholding exist, such as those listed above).

2.5.9 Searching for information

a. The OIA does not specifically define what is considered a ‘reasonable search’.

b. Before applying s 18(e) of the OIA (refusing a request on the basis that the information does not exist or cannot be found) a record detailing the search for information is to be compiled, including (where relevant) searches of—

(1) hard copy files (desks, filing cabinets and storage sites, both internal and external to NZDF facilities, including archives);

(2) records management systems and other databases;

(3) computer drives and files (including personal drives and files where necessary);

(4) email accounts;

(5) text messages (where accessible);

(6) portable storage devices;

(7) mobile phones, tablets and other portable ICT equipment (official and personal) where accessible;

(8) home computers where staff may be working remotely and where accessible;

(9) website announcements and information promulgated on the NZDF intranet and internet;

(10) notepads, diaries and electronic calendars;

(11) digital imagery; and

(12) audio and video recordings.

c. All this information potentially falls within the scope of an OIA request.

d. While most NZDF information is created and archived electronically, the volume of information stored has increased as draft versions of documents, multiple copies of the same document, emails and supporting information downloaded from the web are automatically stored within the digital information environment. A search for information within the document management system and that archived in paper-based files may be a challenge when researching and collating information.

e. When undertaking electronic searches for information, key words and other search terms used to locate the information should be recorded for future reference for similar enquiries or an Ombudsman's investigation.

Section 3 - Responding to requests for information

2.5.10 Headquarters New Zealand Defence Force

a. Within HQNZDF—

(1) The **CoS HQNZDF** is responsible for managing all requests for access to official information made directly to HQNZDF or through the 'media gateway', and requests referred to the OCDF by other parts of the NZDF or transferred to the NZDF;

(2) The **Director Defence Public Affairs (D DPA)** is responsible to the CoS HQNZDF for responding to requests for access to official information made through the media gateway.

(3) The D DPA must refer a request for access to official information to the CoS HQNZDF when a response may—

(a) impact on the reputation of the NZDF;

(b) require consultation with other parts of the NZDF;

(c) involve the research and collation of a large amount of information;

(d) require consultation with DLS;

(e) require review by the Chief Financial Officer (CFO);

(f) involve sensitive information concerning the defence and security of New Zealand and its people or the government's international relationships; or

(g) require considered application of the PA.

(4) The **Chief People Officer (CPO)** is responsible to the CoS HQNZDF for ensuring that—

(a) requests by persons for access to their service records or record of employment are properly administered; and

(b) all requests for access to official information made to Veterans' Affairs, with the exception of requests for service records, are referred to the OCDF (Ministerial Services).

(5) **Chiefs of Service (COS)** may respond to requests for official information.

(6) Requests made directly to the Vice Chief of Defence Force, the CFO, the Chief of Joint Defence Services and the Chief Defence Strategy Management must be referred to the CoS HQNZDF.

2.5.11 Headquarters Joint Forces New Zealand

a. The Commander Joint Forces may respond to requests for official information made directly to Headquarters Joint Forces New Zealand (HQJFNZ) concerning current operations, operational activities in support of public service agencies and other tasks being conducted under the command and control of the Commander Joint Forces.

b. A request for access to official information must be referred to the CoS HQNZDF when a response may—

(1) impact on the reputation of the NZDF;

(2) require consultation with other parts of the NZDF;

(3) involve the research and collation of a large amount of information;

(4) require consultation with DLS;

(5) require review by the CFO;

(6) involve sensitive information concerning the defence and security of New Zealand and its people or the government's international relationships; or

(7) require considered application of the PA.

c. The Commander Joint Forces must appoint an Information Contact Officer to administer requests for access to official information and ensure that this officer is trained on the NZDF policies and procedures, and the requirements of the OIA and the PA.

d. The Commander Joint Forces must ensure that all requests for access to official information are properly recorded. The Corporate and Ministerial Services Team will contact Commander Joint Forces for the data when reporting to the Public Service Commission is required.

e. Where doubt exists concerning a response to a request for official information, the Commander Joint Forces must refer the request to the OCDF.

2.5.12 Service-arms, bases, ships and camps

a. COS may respond to requests for official information made directly to their personnel, bases, camps and ships concerning the Navy, Army or Air Force and other tasks being conducted under the command and control of the relevant Chief of Service. COS are to promulgate orders, consistent with this DFI, for the administration of requests for official information.

b. A request for access to official information must be referred to the OCDF when a response may—

(1) impact on the reputation of the NZDF;

(2) require consultation with other parts of the NZDF;

(3) involve the research and collation of a large amount of information;

(4) require consultation with DLS;

(5) require review by the CFO;

(6) involve sensitive information concerning the defence and security of New Zealand and its people or the government's international relationships;

(7) require considered application of the PA; or

(8) when considering charging the requester for release of the information.

c. COS must ensure that Information Contact Officers are appointed in bases, camps and ships authorised to respond to requests for official information. Information Contact Officers are to administer requests for access to official information and must be trained on the NZDF policies, procedures and the requirements of the OIA and the PA.

d. COS must ensure that all requests for access to official information are properly recorded. The Corporate and Ministerial Services Team will contact COS for the data when reporting to the Public Service Commission is required.

e. Instructions for the handling of requests for access to official information are prescribed in *Annex 2-C*.

f. Where doubt exists concerning a response to a request for official information, a COS or designated Information Contact Officer must refer the request to the OCDF.

2.5.13 Processing requests for official information

a. Processing requests for access to official information is a legislative obligation placed on the NZDF. For each request, the provisions of the OIA expects the organisation to—

(1) respond within the statutory time limit;

(2) locate, collate and review all the information and material requested;

(3) consider the impact of the release of the information;

(4) seek the advice and consult third parties where required;

(5) prepare the information for release or provide clear and unambiguous reasons why it will not be made available; and

(6) ensure that the person making the request is advised of their right of review of any decision by the Ombudsman.

b. One of the purposes of the OIA is to progressively increase the availability of official information to the public, but it is not intended to be the sole means by which the public can find out about the activities of the government.[38]

c. The public or media may seek information from the NZDF for a range of purposes and typically for—

(1) details about a particular event or incident;

(2) personal interest;

(3) reporting on matters they consider to be in the public interest;

(4) research;

(5) general interest in a particular issue; and

(6) performance matters.

d. The NZDF voluntarily promulgates a significant amount of information and other material in print and web-based formats for the benefit of the public. Often this information is in sufficient detail to satisfy the interest of the public in NZDF activities.

2.5.14 Dealing with requests for information

a. The OIA makes provision for a number of legislative requirements when dealing with requests made under the OIA as follows—

(1) **Response time**. The requester must be advised of a decision on the request as soon as reasonably practicable and no later than 20 working days after a request has been received.[39] The working day count starts on the first working day after a request has been received.

(2) **Transfers**. Where the NZDF does not hold all of the information or the request would be more properly answered by another entity, the request is to be transferred to that organisation no later than 10 working days after receipt of the initial request.

(3) **Extensions of time**. When considering a request to the NZDF, the CoS HQNZDF may extend the time limit for a reasonable period of time if—

(a) the request is for a large amount of information and meeting the timeframe would interfere with the operations of the NZDF;

[38] OIA, s 4(a).

[39] Section 11 of the *Electronic Transactions Act 2002* refers to time of receipt. An electronic communication is taken to be received when (a) the time the communication enters the information system (eg email or website irrespective of whether it is outside normal working hours of the agency), or (b) in any other case, at the time the electronic communication comes to the attention of the addressee.

(b) the request requires a search through an extensive amount of information and meeting the timeframe would interfere with the operations of the NZDF; or

(c) consultations are required and a proper decision cannot be made within the original time limit.

(4) **Responses to requests**. A response to a request for information should be complete and provide sufficient information in order to provide context and understanding.

(a) While the format and way the information is made available is the preference of the requester, the NZDF response to a request for official information will normally be provided electronically.

(b) Responses to requests for official information should be sent under a covering letter and—

(i) by email to the requester at the original email account provided to the NZDF; or

(ii) posted in hard copy and addressed personally to the requester.

(c) Documents or the information requested are to be watermarked 'Released under the Official Information Act 1982'.

(d) Where providing the information in the form requested would impair the efficient administration or unduly interfere with the operations of the NZDF; there is a significant amount of documentation; or where there are controls on the release of certain material, a person requesting official information may be—

(i) invited to inspect the documents or information at an NZDF facility;

(ii) invited to view audio or visual material;

(iii) furnished with a written transcript of a meeting or document that has been recorded in another language or shorthand;

(iv) offered an excerpt or summary of the contents of the document(s); or

(v) furnished with an oral presentation of the information sought.

(e) Should the information not be provided in the format requested, the NZDF must notify the person making the request as to the reasons why.

(f) Responses to requests made by the media or public through the 'media gateway' are normally returned by email and should be unambiguous. Responses are to be written in plain English and address the specific enquiry.

(g) While it is expected that the public will normally explore the internet or other written material for information before making a request, a fair and reasonable response may be to direct the person to any previously published material in the public domain.

(5) **Identification of third-party details**. Any information in a response that could identify a third-party individual or group of persons should not be included unless it is already publicly available or express permission to provide the information is granted; this may include identification by name, contact details (including email accounts) or any other personal information.[40]

(6) **Deletions and redactions in documents**. Where some information in a document is to be withheld, the releasing officer may approve text to be redacted. All redactions must comply with the provisions for withholding access to the information.[41] Approved redaction software applications must be used for making redactions and deletions in documents being prepared for release.[42]

(7) **Refusal of requests**. A request may be refused in full or in part, pursuant to s 18 of the OIA. If a request is likely to be refused, the requester should be consulted and offered an opportunity to reconsider the request or present it in a way that would remove the reason for a refusal. The requester must be kept informed of the progress of the request for access to official information when—

(a) the request has been received;

(b) the request has been transferred;

(c) an extension of time has been applied (with reason for the extension); and

(d) an alternative means of satisfying the request is being offered or considered.

b. All communications with requesters must be respectful and provide clear and unambiguous responses.

c. Decisions to provide access to official information must be appropriate to the provisions of the OIA and communicated to the requester as soon as reasonably practicable and in accordance with the statutory timeframes. The identity of the requester, their means of engagement or any other practices must not affect the proper release of the information requested.

d. If there is doubt as to the information being sought or potential challenges in researching or collating the material, the requester is to be consulted before refusing to make information available. It is not permitted to decline requests on the basis that the information is too time-consuming to collate without offering the applicant an opportunity to refine the scope of the request.

e. Should a person requesting access to official information later amend the original request, the request is to be considered as a new request that replaces the original request. The time count for a response starts on the first working day following receipt of the amended request. This circumstance does not apply if the NZDF seeks clarification of the request from the requester after 7 working days.[43]

[40] PA, pt 3, sub-pt 1, s22, Information privacy principle 11.
[41] OIA, ss 6, 7, 9 and 18.
[42] Approval level for Ministerial Services and for OIA purposes – CoS HQNZDF.
[43] OIA s 15(1AB).

2.5.15 Characterising requests made under the Official Information Act 1982

a. Before any response to a request for access to official information is prepared, it must be determined whether the OIA or the PA is to be used. The flowchart at Figure 2-1 provides a means of determining the appropriate governing statute.

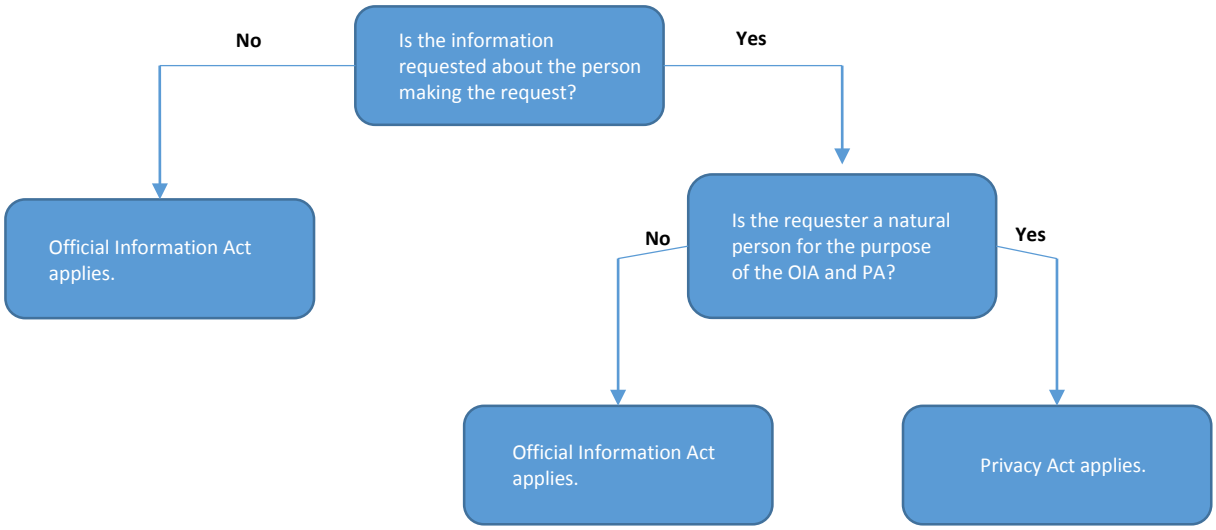

Figure 2-1 – Determining which statute applies to requests for information

b. A request by a company (or any other entity that is not a natural person) for information about the NZDF or a request by a person for information about a member of the NZDF (unless they are that person's representative) is to be considered under the OIA.

c. Any information requested by a natural person about themselves is to be considered under the provisions of the PA.

d. There may be occasions where access to official information must be considered under both the OIA and the PA. The OIA does not have primacy over the PA; care must be taken to ensure that personal privacy is protected at all times.

e. Where there is doubt about the application of this section, then the Corporate and Ministerial Services team or the local DLS officer are to be consulted.

2.5.16 Accessibility and usability of official information releases

a. Each release of official information must be considered in the context of previous releases to ensure that any approach taken to a response is consistent. This must also include reconsidering documents already publicly available and identifying other information for release or promulgation on the NZDF website.

b. Documents and material made available to an applicant in response to a request for access to official information must be those originally communicated and not a more recently altered or amended version. Documents and material supplied should also normally be returned in the format requested by the applicant but there may be

occasions where this is not possible.[44] In cases where video and digital images are to be used, take care to review any geolocation and metadata to ensure information that should not be released or is out of the scope of the request is not inadvertently released.

c. Typically, responses will be provided in text-searchable portable document format (pdf).

2.5.17 Withholding access to official information

a. The NZDF may withhold all or part of any material requested and may refuse a request for information for good reasons.[45]

b. Where a request for information is refused, the applicant should be advised of the reason and informed of their right to seek a review of the decision on their request by the Ombudsman.

c. A security classification or endorsement does not in itself provide good reason for withholding official information. The security classification or endorsement determines how a document is handled within the government system.

d. A decision to withhold any information that is classified or is protected by special handling endorsements must be made under the criteria of the OIA, as for all other official information. However, a high-level security classification or endorsement may provide a useful flag, indicating that there may be good reason for withholding the information (or part of it) under the provisions of the OIA.[46]

2.5.18 Conduct of the review by the Ombudsman

a. A person who has requested official information can ask the Ombudsman to investigate a decision by the NZDF regarding their request.[47] These reviews by the Ombudsman are commonly referred to as 'investigations into complaints to the Ombudsman'.

b. Where the Ombudsman undertakes a review, the NZDF must comply fully with the requirements of the OIA. The Ombudsman will not be content to accept superficial assertions or the use of a blanket provision, such as 'free and frank advice', to justify not releasing information. The NZDF must provide a detailed justification in each case and should use the review as an opportunity to set out any concerns about the request.

[44] OIA, s 16(2).
[45] An agency can refuse a request or withhold information if there is a good reason to do so under the OIA. Reasons for withholding information and refusing a request are in ss 6, 7, 9 and 18 of the OIA and fall into the broad categories of: conclusive reasons to withhold; other reasons to withhold balanced against the public interest; and refusing requests. Refer to the OIA for the details. Guidance on how to use these sections can be found on the Office of the Ombudsman website.
[46] OIA, ss 6,7,9 and 18.
[47] OIA, pt 5.

c. The Ombudsman has extensive powers to request information for the purposes of the review.[48] The NZDF must respond within 20 working days to any such request. The time limit for responding may be extended by notice to the Office of the Ombudsman.

d. Any reviews by an Ombudsman are managed by the Corporate and Ministerial Services team.

2.5.19 Ombudsman's recommendation

a. An Ombudsman, having investigated a complaint made under the OIA, will issue an opinion and may make such recommendations as they see fit.[49] If an Ombudsman considers that the original request should have been met or that an unreasonable decision was taken, the Ombudsman will recommend to CDF the action to be taken.

b. Before making a recommendation, it is the Ombudsman's practice to first provide the NZDF with a provisional opinion for comment and to arrange for any other affected party to be consulted. The Ombudsman may also offer to discuss personally any case where their opinion differs from that of the holder of the information.

c. The NZDF must respond to an Ombudsman's recommendation within the timeframe outlined.[50]

d. Once a final opinion is received, the decision must be promulgated within the OCDF and to other decision-makers to ensure compliance.

2.5.20 Performance and monitoring

a. Well-organized record-keeping and information management policies and systems are fundamental enablers for compliance with the OIA and the effectiveness of the organisation's administrative practices.

b. Monitoring the organisation's performance in responding to requests for access to official information, providing consistent and quality responses and managing the workload of the staff involved necessitates robust processes and the means of ensuring that the provision of information is complete and reliable. This can be achieved by recording relevant data with respect to each request including calls for information from the media.

c. The recording of information about requests for access to official information should include—

(1) type of request (refer to parts 2, 3, and 4 of the OIA);

(2) the actual wording of the request (and interpretation of the request if ambiguous);

(3) previous or related requests for information;

(4) name of the requester and organisation being represented;

(5) the time of receipt of the request;

[48] *Ombudsmen Act 1975*, s 18.
[49] OIA, s 28.
[50] OIA, s 28.

(6) if the request was transferred and the reason(s) why;

(7) other public service agencies consulted;

(8) if the timeframe for a response was extended and by how long;

(9) the outcome of the request ('granted in full', 'granted in part' or 'refused in full');

(10) details of any information withheld and under which provisions of the OIA;

(11) details of the search for information;

(12) whether the minister was consulted on the decision to release the information;

(13) whether the decision was notified to the minister;

(14) whether the NZDF charging regime was applied;

(15) date of release of the official information to the requester and by what means; and

(16) total time taken to answer the request.

2.5.21 Documenting requests made through the media gateway

a. All requests for official information made through the media gateway must be documented.

b. For analysis and reporting purposes, information must be recorded in an exploitable database and made available to Ministerial Services. For all individual requests for information made through the media gateway the following information must be recorded—

(1) receipt date/time group;

(2) name and organisation of the requester;

(3) information requested;

(4) information provided; and

(5) response date/time group.

c. For all enquiries for information made through the media gateway, the following information is to be recorded and reported to Ministerial Services—

(1) total number of requests received;

(2) number of requests responded to within 20 working days;

(3) number of requests not responded to within 20 working days; and

(4) number of requests refused (including requests that receive no response).

2.5.22 Managing records of requests for official information

a. Records regarding requests for official information must be routinely analysed by the CoS HQNZDF, and outcomes reported to CDF, COS and senior executives as appropriate.

b. The information arising from the analysis of requests has three outcomes. It allows the organisation to—

(1) be aware of potential issues that may be in the public interest and for which there may be further enquiries;

(2) be cognisant of the performance of the internal OIA processes and recommendations of the Ombudsman; and

(3) improve the management of the NZDF official information processes and training modules.

c. The analysis and reporting is to include emerging trends or questions about a particular subject, frequency of requests, opportunities for the voluntary release of information and the results of any Ombudsman investigations.

d. The recording and examination of requests for information must include enquiries made through the media gateway, requests made directly to the Services and HQ JFNZ, and requests for personal information contained in Service records or records of employment. Instructions related to recording this information are prescribed in this publication.

e. Ministerial Services must be kept informed of requests for official information handled by COS and the D DPA in order to indicate trends in public interest of noteworthy matters in order to pre-empt further requests on the same or similar issue.

f. The total number of requests for access to official information must be made available for publishing in the *NZDF Annual Report* to Parliament. This total must include all requests received by all parts of the NZDF.[51]

2.5.23 Voluntary release of information

a. Official information may be released proactively.

b. The OIA does not direct or prohibit the voluntary or proactive release of official information. There can be significant advantages in voluntarily publishing information that may be of interest to the public. Opportunities for the planned publication of information to assist the public's understanding of the NZDF and the organisation's activities and reduce media speculation should be considered wherever practicable.

c. It is in the best interest of the NZDF to voluntarily and routinely publish a range of information that may be of interest to the public on the NZDF website.

d. The extent and variety of information should include—

(1) business documents such as—

(a) Statements of Intent;

(b) Four-Year Plans;

(c) Annual Reports to Parliament;

(d) briefings to an incoming minister; and

[51] In particular: Ministerial Services, DPA, Service-arms, Joint Forces, Veterans' Affairs, bases, camps and ships.

(e) register of gifts and hospitality.

(2) information relating to the functions of the NZDF;

(3) strategy, planning and performance reports (where not protected under the auspices of the *Protective Security Requirements*);

(4) current activities;

(5) media releases;

(6) information about the material the NZDF holds;[52]

(7) responses to requests for access to official information;

(8) a record of information provided to media and the public;

(9) information about external or regulatory reviews conducted by other agencies;

(10) investigative reports that are of public interest;

(11) defence-related articles in journals of a general interest, including Service periodicals; and

(12) results of disciplinary events (where permitted).

e. The CoS HQNZDF identifies opportunities for voluntary or proactive release of information that is of interest to the public; eg where a high number of requests for access to official information has been received about a particular subject. On occasions, it may be appropriate to host a press conference to provide information to a wide audience.

f. In accordance with government directions, Cabinet papers (with a few exceptions) are to be published publicly. For Defence and Veterans' Affairs papers, these are available on either the NZDF, Veterans' Affairs or Ministry of Defence OD websites as appropriate on behalf of the Minister of Defence and Minister for Veterans. The Corporate and Ministerial Services team is responsible for the preparation and posting of Cabinet papers on the NZDF website, as appropriate/required.

g. All-of-government guidance on the proactive release of official information may be found on the *Public Services Commission* and *Ombudsman* websites.

2.5.24 Rules for the voluntary release of official information

a. Information that may be suitable for proactive release includes policies and procedures, research, reports, material that would help the public best understand the role of the NZDF and other material of general interest that may become subject to requests under the OIA.

b. The following matters should be considered before a person with a delegated authority to approve the voluntary release of official information publishes the material online. That person must—

(1) apply the principles in the OIA, the PA, and the *Protective Security Requirements* to the information;

[52] OIA, s 20.

(2) determine whether the document contains any information that would have been withheld if the information had been requested under the OIA;

(3) determine whether the document contains any information that must be withheld under the terms of any other legislation (eg the *Armed Forces Discipline Act 1971*); and

(4) decide whether, in the circumstances, publication on the website is the best means of public release.

c. Section 48 of the OIA protects agencies from civil or criminal sanctions when releasing official information in good faith in response to a request for information.

d. Persons authorised to promulgate official information on the NZDF website must undertake due diligence and consider any potential liability that might result from the proactive release of official information or as a consequence of publication (eg defamation or breach of contract) before deciding to publish the information. If any doubt exists, the advice of DLS must be sought.

2.5.25 NZDF official information webpage

a. All official information promulgated on the NZDF website and NZDF official information webpage must conform to the New Zealand Government's *Web Accessibility Standards*. Website managers must follow these standards when preparing material for promulgation on the external-facing NZDF website, as the standards are subject to change without notification.

b. The NZDF official information webpage is controlled by the CoS HQNZDF. Changes to the website itself and promulgation of official information on the NZDF website must be approved by the CoS.

c. The design and format of the NZDF webpage must allow persons to request access to official information without difficulty and provide clear guidance on how the NZDF will respond to their requests. This webpage is to be—

(1) available directly from the NZDF homepage;

(2) separate from the NZDF 'Contact us' page; and

(3) available in te reo Māori.[53]

2.5.26 Considering a request

a. The NZDF must make and communicate a decision on any request received as soon as reasonably practicable and no later than 20 working days after it was received. Depending on the extent of a request an extension of time to deal with a request may be sought.

b. **Extensions.** The NZDF may extend the maximum time limit for making a decision, for a reasonable period, if—

(1) the request requires a search through a large quantity of information; or

[53] Availability in te reo Māori is under development.

(2) consultations to inform a proper response could not be completed within the initial time period.

c. The NZDF must notify the requester of an extension within 20 working days and—

(1) specify the period of the extension;

(2) give the reasons for the extension; and

(3) advise the requester of the right to seek a review by the Ombudsman about the extension.

d. **Urgency**. A request for information may be treated as urgent and, if so, the requester must give reasons for seeking the information urgently. The NZDF will decide whether it is reasonable to give priority to a request over other requests for information and existing work.

e. **Transferring a request**. The NZDF will transfer a request for official information when—

(1) the information is not held by the NZDF, and it is believed that the information requested is held by another agency; or

(2) it is believed that the request is more closely connected to another agency.

Any decision to transfer a request for information must be advised to the requester within 10 working days of receiving the request.

f. **Publication of responses.** The NZDF may publish responses to requests for information (with personal information removed) on the NZDF website. Requesters will be notified of this when the decision on a request is provided.

2.5.27 Charging for official information

a. Usually, there will be no charge for providing information in response to a request made under the OIA.

b. If there is a substantial cost to the NZDF for providing information, a requester may be asked to meet some or all of the costs. A charge for information may result from the cost of labour and materials involved in making the information available, including responding to requests under urgency or a need to engage additional staff.

c. If there is to be a charge, the requester will be advised of the estimate of the charge and given the option to continue or not with the request. The NZDF may request that the charge or a deposit be paid before the information is released.

d. The final decision to charge a requester for the provision of official information rests with the CoS HQNZDF. Any request where charging is being considered must, therefore, be forwarded to the Corporate and Ministerial Services team, OCDF.

e. The Ministry of Justice issues guidelines for applying reasonable charges for the purposes of the OIA. The Office of the Ombudsman also publishes guidance on charging regimes. The guidelines are promulgated on the departmental websites.

f. These guidelines must be followed in all cases unless good reasons exist for not doing so.

g. The NZDF instructions for the charging for official information are—

(1) a charge will only be considered if—

(a) the total amount of staff time spent searching for and retrieving the requested information, providing transcripts and supervising access exceeds one hour;

(b) the number of A4-sized pages provided is or will be in excess of 20; or

(c) additional items are required when providing the information (eg DVDs/CDs, flash drives, etc) and a direct charge is incurred.

(2) staff time will be charged at a rate of 38 dollars per half hour (after the first hour);

(3) paper will be charged at a rate of 20 cents per A4 page after the first 20 A4 pages; and

(4) additional items will be charged at an amount that recovers up to the actual costs involved.

h. The decision to charge a fee for the provision of official information must not be made solely on the basis that there may be substantial research or collation work in responding to a request.

i. Charging requesters cannot be used as a deterrent to making requests and avoiding the provision of official information.

j. If charging a requester is appropriate, then the requester must be informed of the likely cost before the information is released.

2.5.28 Complaints

a. If a person is concerned about the way a request has been handled or is dissatisfied with the NZDF's response, they may—

(1) contact the NZDF in the first instance and seek to resolve the issue immediately; or

(2) make a complaint to the Office of the Ombudsman.

b. Concerns may include—

(1) refusing a request;

(2) withholding all or part of the information from release;

(3) failure to meet the timeframe for a response;

(4) extending a timeframe for making a response; or

(5) charging for providing the information.

c. A complaint to the NZDF or to the Ombudsman should be made in writing.

d. The Ombudsman will decide whether to investigate and review any decision made by the NZDF, and may make a recommendation on resolving the complaint.

e. *Annex 2-C* provides guidance for persons making a request for access to official information.

Annexes to Chapter 5

ANNEX 2-B

GUIDELINES FOR ENGAGING WITH MINISTERS

1. These guidelines refer to both how the NZDF is to manage requests for access to official information involving ministers, as well as the conventions for keeping ministers informed of both requests for and the release of information by the NZDF.

2. While the OIA places separate statutory obligations on ministers and chief executives regarding the release of official information, CDF (as a chief executive) has a responsibility, in part, to the appropriate minister for the stewardship of the NZDF and the tendering of free and frank advice to ministers and successive governments.[54] Further advice can be found in *Cabinet Manual 2017*.

Ministers' interest in requests for official information

3. Ministers of the Crown have the ultimate responsibility for the public service agencies within their portfolios.[55] Given that accountability for departmental actions rests with the minister, they may have a legitimate interest in any information requested from their department, as they may need to prepare for the possibility that the release of official information will result in public or political commentary for which they are expected to act in response.

4. While regulating the criteria for releasing information, the OIA is also about protecting official information consistent with the public interest. This level of protection extends to protecting the Government's interests and withholding information (eg that relating to the security and defence of New Zealand and the Government's international relationships). Ministers may have a different and justifiable opinion (particularly when it comes to protecting international relationships) about a response to a request for information. Therefore, the correct processing of a request and assessment of likely withholding grounds may require ministerial consultation.

Notifying ministers of requests for information

5. It is a reasonable expectation that the NZDF notifies the minister(s) of requests for information that may involve their interests.

   a. **'No surprises'**. The 'no surprises' concept adopted by the Government means notifying minister(s) about decisions that the NZDF has taken to release official information. It means informing ministers of matters of significance within their portfolio responsibilities without undue delay, especially where these matters may be controversial or may become the subject of public debate.

   b. The Minister is notified of requests for access to official information received by the NZDF in the *Defence Minister's Weekly Report.*

   c. If the minister's input or opinion is required this should be conducted under consultation.

[54] *State Sector Act 1988*, s 32.
[55] Cabinet Manual 2017 para 2.22-3.

d. If the minister needs to make a decision on a request, the request should be transferred to the minister.

6. **Consultation**. Consultation is the means by which CDF may seek the minister's input to a request before the information is released.[56] Consultation is discretionary and not a statutory obligation. Consultation is appropriate when a minister's input is required before making a decision to release particular information. There is no requirement to consult the minister on all requests for information.

a. Consultation is a formal process of discussing matters concerning a particular subject with others in order to get their advice or opinion. Consultation is not negotiation. In this context, the NZDF must consider the minister's input on a request for information in good faith before deciding whether that input provides reasonable grounds for changing the proposed decision on the request.

b. It is reasonable to consult the minister when the release of information could be of concern to the minister because—

(1) they provided the information;

(2) it is about their role or functions;

(3) it could affect their role as minister; or

(4) the release of information may generate political or media opinion.

c. In consulting the minister, the NZDF must provide the minister with sufficient time to provide appropriate input in relation to the proposed decision to release the information. The minister is to be consulted on the proposed response as soon as reasonably practicable.

d. Appropriate ministerial input includes comments on—

(1) the proper application of withholding grounds and the public interest test;

(2) the release of additional information that the NZDF may not be aware of, including information that may add to the context of the response; and

(3) the proactive release of the same information to others, provided there is no delay in providing that information to the requester.

e. It is not appropriate to—

(1) provide irrelevant information to avoid political embarrassment;

(2) withhold official information without any proper statutory basis; or

(3) act in any way contrary to the provisions of the OIA.

f. While the NZDF is permitted to extend the maximum timeframe for making a decision on a request, any consultation with the minister should not, under normal circumstances, exceed the requirement for CDF to respond to a request for information within 20 working days. Applying an extension of time for a response should be the exception not the rule.

[56] OIA, s 15(5).

g. Having received the minister's input, if there is a disagreement as to the proposed decision to release information, CDF will decide whether to transfer the request to the minister or respond to the request.

h. CoS HQNZDF must keep an accurate record of all consultations with ministers in relation to requests for information.

7. **Transfer of a request to the minister**. Transferring a request for information to the minister moves the responsibility for decision-making on the request to the minister. This ensures that the decision on release or withholding of any information is made by the person best placed to make that decision.[57]

a. The decision whether or not to transfer the request must be made in consultation with the minister's office. A record of the consultation must be kept.

b. The decision to transfer a request to the minister must be made on the specifics of the information requested, not the identity of the requester or their organisation, the degree of controversy or sensitivity of the subject matter, or any other factor.

c. There should be a reasonable basis for transferring the request to the minister, such as —

(1) it is more closely connected to the minister's functions;

(2) the minister holds the information; or

(3) it involves Cabinet material from that minister's Government.

d. A transfer to the minister must be made within 10 working days from first receiving the request. Once the request is transferred, the working-day time count for responding starts afresh from the day after the request is transferred.

e. The NZDF should share any relevant information regarding the request with the minister.

f. The NZDF must advise the requester of the transfer and the reasons for the transfer.

[57] *Cabinet Manual 2017*, para 8.34.

ANNEX 2-C

GUIDANCE FOR PERSONS MAKING A REQUEST FOR ACCESS TO OFFICIAL INFORMATION[58]

1. Under the OIA, individuals may ask for information held by the NZDF.
2. Information held by the NZDF includes, but is not limited to—
   a. information concerning the activities of the NZDF, the Services (Navy, Army, and Air Force), joint operations, Veterans' Affairs;
   b. information concerning internal policies, processes, rules or guidelines;
   c. advice provided to the Government; and
   d. information we may hold about you and/or your time in the NZDF.
3. Requests should be specific about the information required. In most cases individuals should be provided with the information requested. However, where applicable, some information may be withheld to—
   a. protect the security and defence of New Zealand;
   b. protect the safety of any person;
   c. comply with the law;
   d. protect the privacy of individuals;
   e. protect information that is commercially sensitive or provided in confidence;
   f. protect legal professional privilege; and/or
   g. maintain the effective conduct of the decision-making and policy advice processes of government.
4. Unless specifically requested, the contact details for members of the NZDF are withheld to avoid malicious or inappropriate use of staff information.
5. Requests should be made in writing and can be made by—
   a. using the *NZDF Contact Form* on the NZDF website;
   b. by email to *ministerialservices@nzdf.mil.nz*; or
   c. in writing to:

      Office of the Chief of Defence Force
      Headquarters New Zealand Defence Force
      Private Bag 39997
      Wellington Mail Centre
      Wellington 5045

[58] Available on the NZDF Web page.

6. If you are not satisfied with a decision concerning your request for information, you can *contact the Office of the Ombudsman* to seek a review of that decision.

Considering a request

7. The NZDF will make and communicate a decision on your request as soon as reasonably practicable and no later than 20 working days after it is received. Depending on the extent of a request, the NZDF may seek an extension of time to deal with a request.

8. **Extensions.** The NZDF may extend the maximum time limit for making a decision, for a reasonable period, if—

   a. your request requires a search through a large quantity of information; or

   b. consultations to inform a proper response could not be completed within the initial time period.

9. The NZDF will notify you of an extension within 20 working days and—

   (1) specify the period of the extension;

   (2) give the reasons for the extension; and

   (3) advise the requester of the right to seek a review by the Ombudsman about the extension.

10. **Urgency.** A request for information may be treated as urgent, and if your request is urgent you must give reasons for seeking the information urgently. The NZDF will decide whether it is reasonable to give priority to a request over other requests for information and existing work.

11. **Transferring a request.** The NZDF will transfer a request for official information when—

    a. the information is not held by the NZDF, and the NZDF believes that the information requested is held by another agency; or

    b. it is believed that the request is more closely connected to another agency.

    Any decision to transfer a request for information will be advised to you within 10 working days.

12. **Publication of responses.** The NZDF may publish responses to requests for information (with personal information removed) on the NZDF website. You will be notified of this when the decision on a request is provided.

Charging for information

13. Usually, there will be no charge for providing information in response to a request made under the OIA.

14. If there is a substantial cost to the NZDF for providing information, you may be asked to meet some or all of the costs. A charge for information may result from the cost of labour and materials involved in making the information available, including responding to requests under urgency or a need to engage additional staff.

15. If there is to be a charge, you will be advised of the estimate of the charge and given the option to continue or not with the request. The NZDF may request that the charge or a deposit be paid before the information is released.

Complaints

16. If you are concerned about the way a request has been handled or are dissatisfied with the NZDF's response, you—

    a. should contact the NZDF in the first instance and seek to resolve the issue immediately; or

    b. can make a complaint to the *Office of the Ombudsman*.

17. Concerns may include—

    a. refusing a request;

    b. withholding all or part of the information from release;

    c. failure to meet the timeframe for a response;

    d. extending a timeframe for making a response; or

    e. charging for providing the information.

18. A complaint to the NZDF should be made in writing and can be sent to the OCDF—

    a. by email to *ministerialservices@nzdf.mil.nz*; or

    b. in writing to—

    Office of the Chief of Defence Force
    Headquarters New Zealand Defence Force
    Private Bag 39997
    Wellington Mail Centre
    Wellington 5045

19. A complaint to the Ombudsman should be made in writing and can be submitted—

    a. using the *online complaint form*;

    b. by email to *info@ombudsman.parliament.nz*; or

    c. in writing to—

    The Ombudsman
    PO Box 10152
    Wellington 6143

20. The Ombudsman will decide whether to investigate and review any decision made by the NZDF and may make a recommendation on resolving the complaint.

Chapter 6 - General Inquiries and Media Requests

2.6.1 General inquiries from the public and the media

a. General inquiries from the public and requests for information from the media are subject to the provisions of the *Official Information Act 1982* (OIA) and, where relevant, the *Privacy Act 2020* (PA).

b. Requests from the media are often related to checking facts or confirmation of information already known. On occasion, the media and the public may seek information about an activity or event that they may consider to be of public interest.

c. Inquiries of this type are normally made via the 'media gateway'.

2.6.2 Media gateway

a. The public and representatives from New Zealand media organisations may request official information from the New Zealand Defence Force (NZDF) through the media gateway. A link to the media gateway is to be provided on the NZDF official information webpage.

b. Responses to media and public inquiries must be accurate, unambiguous and provided to the individual requester as soon a reasonably practicable. To avoid the possibility of misreading a response, it is preferable that the response to a request for official information made through the media gateway is made by email.

c. Where there is a need to research or collate a response, the requester must be informed of the need and of an approximate timeframe for the answer to their query.

d. If it is considered that the request for information requires substantive research or a detailed response, or the subject is sensitive, the requester is to be informed that the request for information will be referred to Ministerial Services for their attention.

e. If the decision is to decline to provide the information, the requester must be informed of the reasons and advised that they may complain to the Ombudsman and request a review of the decision.

f. At no time must the identity of the requester or their organisation be the cause of treating a request for information from the media or public differently.

g. Members of the NZDF must not refuse access to information requested by the media because of the potential for misreporting, misleading headline-making or selective reporting of the information released.

h. Enquiries from the public and media dealt with through the media gateway must be fully documented, and records must be submitted to Ministerial Services Headquarters New Zealand Defence Force (HQNZDF) for inclusion in the reporting of requests made pursuant to the OIA and the PA.

2.6.3 General enquiries not made through the media gateway

All requests for official information not made through the media gateway must be fully documented and submitted to the Chief of Staff (CoS) Headquarters New Zealand Defence Force (HQNZDF) (Ministerial Services).

2.6.4 Persons may seek information about themselves

a. Persons may seek access to information held by the NZDF about themselves.[59]

b. This information may be of a general or specific nature and usually found in their personal record of service in the Armed Forces or their employment record in the case of members of the Civil Staff.

c. The request is to be managed in accordance with the provisions of the PA and as prescribed in Part 3 - Implementing the Provisions of the *Privacy Act 2020*.

[59] PA, pt 3, sub-pt, s 22.

Part 3 - IMPLEMENTING THE PROVISIONS OF THE PRIVACY ACT 2020

Chapter 1 - Privacy and Dealing with Information About People

3.1.1 Purpose

a. The *Privacy Act 2020* (PA) promotes and protects individual privacy by providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access and correct their personal information.

b. The PA governs the way that government and private sector organisations must handle personal information. The New Zealand Defence Force (NZDF) must respect individual privacy interests and core privacy principles by ensuring that the collection, storage, management and transmission of information about people is undertaken in accordance with the PA.

c. The purpose of this part is to outline requirements of the PA and detail how privacy is managed with the NZDF.

3.1.2 Information privacy principles

a. The 13 information privacy principles (IPP) are the cornerstone of the PA.[60] The principles are to be used by the NZDF in considering privacy.

b. The principles address how the NZDF may collect, store, use and disclose personal information. They also allow an individual to request access to personal information about themselves and to correct that information. The IPP in brief are as follows—

(1) **Principles 1–4** relate to the purpose, source, collection and manner of collection of personal information.

(2) **Principles 5–9** cover storage and security of personal information, access to personal information, correction of that information and the accuracy of information.

(3) **Principle 10** defines limits on the use of personal information.

(4) **Principle 11** limits the disclosure of personal information.

(5) **Principle 12** covers disclosure of personal information outside New Zealand.

(6) **Principle 13** covers the use of unique identifiers.

c. The Privacy Commissioner issues *Codes of Practice* that may modify the operation of the PA for specific industries, agencies, activities or types of personal information, eg health information. These Codes can modify the application of, or replace, the IPP. These *Codes of Practice* have the force of Regulations and are enforceable through the Privacy Commissioner and Human Rights Review Tribunal.

[60] PA, s 22.

d. All orders, directives and instructions issued by the Chief of Defence Force, or those issued within delegated authorities, including practices relevant to the handling of personal information adopted by members of the NZDF, must comply with the provisions of the PA and any related legislation and governmental direction.

e. The PA came into full effect on 1 December 2020. The new Act repeals and replaces the *Privacy Act 1993*. Key reforms in the new PA include—

(1) **Mandatory reporting of notifiable privacy breaches**. If organisations or businesses have a privacy incident that poses a risk of, or has caused, serious harm, they are required to notify the Privacy Commissioner and affected parties.[61] This change brings New Zealand into line with international best practice.

(2) **Introduction of compliance orders**. The Commissioner may issue compliance notices to require compliance with the PA. Failure to follow a compliance notice may result in a fine of up to $10,000.

(3) **Binding access determinations.** If an organisation or business refuses to make personal information available upon request, the Commissioner will have the power to demand release.

(4) **Controls on the disclosure of information overseas**. Before disclosing New Zealanders' personal information overseas, New Zealand organisations or businesses will need to ensure those overseas entities have similar levels of privacy protection to those in New Zealand, or that the individual concerned is fully informed and has authorised the disclosure.

(5) **New criminal offences.** It is an offence to mislead an organisation or business to obtain access to another person's personal information or have it used, altered or destroyed, or to destroy personal information knowing a request has been made for it.[62] The maximum fine for these offences is $10,000.

(6) **Explicit application to businesses whether or not they have a legal or physical presence in New Zealand.** If an international digital platform is carrying out business in New Zealand, with New Zealanders' personal information, they will be obliged to comply with New Zealand law regardless of where they or their servers are based.

[61] 'Harm' refers to action that has caused, or may cause, loss, detriment, damage or injury to an individual or actions that may adversely affect an individual's rights, benefits, privileges, obligations or interests, causing significant humiliation, loss of dignity and injury to feelings.
[62] PA, s 212(2)(d).

Chapter 2 - NZDF Privacy Policy

3.2.1 NZDF privacy policy

a. The New Zealand Defence Force (NZDF) privacy policy describes the approach that the NZDF employs to manage the personal information entrusted into its care, including risk management processes and those mitigations necessary to ensure the NZDF meets its obligations in safeguarding personal information.

b. The government expects that agencies have policies that[63]—

(1) are aligned with organisational strategy and the *Privacy Act 2020* (PA);

(2) promote a privacy culture that 'operationalises'[64] the concept of 'privacy by design'; and

(3) are owned by a member of the 'Executive Team'.

c. The NZDF Privacy Policy is aligned with the information privacy principles (IPP) outlined in the PA.[65]

d. The *NZDF Privacy Programme roadmap* is issued annually and updated following the GCPO's Privacy Maturity Self-Assessment. The NZDF Privacy Programme roadmap is used as a means through which specific actions can be promoted over the following year to improve privacy maturity.

3.2.2 NZDF management of information

a. The NZDF collects personal information for purposes including command, administration, discipline, security, employment, training, and support for member's health and wellbeing. This information is provided to, and used by, specific members of the NZDF whose duties require them to have access to that information.

b. PA provisions and the IPP apply to personal information throughout its entire life cycle. The information life cycle consists of—

(1) collection;

(2) storage and security;

(3) use;

(4) access and correction;

(5) disclosure;

(6) retention; and

(7) disposal.

c. Personal information collected by the NZDF is retained for the purpose stated and archived under the provisions of the *Public Records Act 2005*. The Chief of Defence

[63] Government Chief Privacy Officer (GCPO) guidance.
[64] For the purpose of this policy, 'operationalise' refers to the management of privacy as part of routine NZDF business.
[65] PA, s 22.

Force (CDF) may determine that there are good reasons to restrict public access to personal information once the information has been archived.[66]

d. Members of the NZDF and other persons employed for NZDF purposes must not use, access, view disclose or destroy any personal information held by the NZDF for any purpose other than in the legitimate course of their duties or as required by law.

3.2.3 Accountability and responsibility for the protection of personal information

a. Every member of the NZDF and other persons engaged for NZDF purposes are responsible for protecting personal information from unauthorised or inadvertent disclosure to non-entitled persons who do not have a legitimate necessary reason for needing to access personal information for a lawful purpose connected with an NZDF function or activity.[67]

b. CDF is accountable to the Government for compliance with the provisions of the PA and other legislative and governmental direction. The Chief of Staff (CoS) Headquarters New Zealand Defence Force (HQNZDF) exercises this obligation on behalf of CDF and maintains direct oversight of all matters of privacy through the NZDF privacy officer.[68]

c. The NZDF privacy officer is appointed by CDF and is customarily the person appointed to the post of Executive Officer, Office of the Chief of Defence Force (XO OCDF). The appointment of a privacy officer is a requirement of the PA.[69]

d. The NZDF privacy officer (a role of the XO OCDF) is also the HQNZDF Unit Security Officer (USO) and manages the appointed HQNZDF USOs to support implementation of security policy and planning and organisation of protective security.[70]

e. The management of privacy within the NZDF is exercised through the network of NZDF USOs[71] in the first instance. Specific privacy leads or champions may also be appointed.

f. The NZDF privacy officer is responsible to the CoS HQNZDF for the proper administration of NZDF privacy policies, the maintenance of the NZDF Privacy Programme roadmap and for ensuring that members of the NZDF are aware of their responsibilities concerning the security of personal information. Specifically—

(1) ensuring compliance with the—

(a) PA; and

(b) NZDF privacy policies and related orders, instructions and directives.

(2) conducting, or having conducted, an initial assessment and/or investigation into an alleged privacy incident where appropriate;

---

[66] *Public Records Act 2005*, s 44.

[67] Non-entitled persons are those without a 'need to know' as defined previously.

[68] The CoS HQNZDF is authorised to promulgate the NZDF privacy policies and investigate privacy complaints pursuant to this DFI as permitted under s 30(2) of the *Defence Act 1990*.

[69] PA, s 201.

[70] Protective security is the protective measures in place to safeguard information, material and personnel appropriate to the threat. See *DFO 51* para 1.9b.

[71] USOs have responsibilities for physical, information and personal security and perform privacy officer responsibilities within this mandate.

(3) working with the Privacy Commissioner in relation to NZDF privacy investigations;

(4) notifying any notifiable privacy breach that poses a risk of serious harm to the people affected by that harm and to the Office of the Privacy Commissioner as soon as practicable;[72]

(5) making information concerning privacy incidents available to Parliament, the Privacy Commissioner and other entities where this does not adversely impact operational security and safety;[73] [74]

(6) making information available to the Privacy Commissioner as the Commissioner may require in the form of reports, assessments and investigations; and

(7) ensuring that the NZDF privacy policies, strategies and programmes are fit for purpose and recommendations are made to CoS HQNZDF for improvements.

g. The NZDF privacy officer expects that USOs and the privacy champions appointed in the various business units of NZDF will carry out the following tasks as appropriate—

(1) Communicate to the NZDF privacy officer any descriptions of privacy breach incidents or near misses, including any action taken to contain breaches and assessments of the incident (relating to incidents that occur within their business unit).

(2) Carry out, as tasked by the NZDF privacy officer, any investigation or privacy impact assessment of the privacy breach incident or near miss.

(3) Undertake a work programme to raise awareness or to ensure compliance with the PA within their business units, as agreed with the NZDF privacy officer.

(4) Undertake projects to raise privacy awareness within their business units on their initiative or as tasked by the NZDF privacy officer.

(5) Undertake further education including attending NZDF privacy meetings, seminars or training arranged by the NZDF privacy officer.

(6) Undertake further education externally on privacy as seen appropriate by the NZDF.

[72] PA, ss 114 and 115.
[73] Eg providing summary reports for the NZDF Annual Report and reports to the Foreign Affairs, Defence and Trade Committee.
[74] Cognisant of any security considerations and requirements.

Chapter 3 - Management of Personal Information

Section 1 - Requests for information

3.3.1 Requests for access to personal information

a. Any member of the public can request information about them held by the New Zealand Defence Force (NZDF).

b. Serving members of the Armed Forces or current employees of the NZDF may request access to information about themselves. These requests are to be made directly to their immediate commander or line manager.

c. Former members of the Armed Forces, former employees of the NZDF, veterans as defined in the *Veterans' Support Act 2014* and their families and any other individual may request confirmation that NZDF holds information about them and may request access to that information. Personal information under the *Privacy Act 2020* (PA) includes personal information of persons who are residing overseas, and, under the PA, requests can be made by individuals residing overseas.[75]

d. Individuals have the right to make a request, and this is enforceable by a court of law.[76]

e. The NZDF must give reasonable assistance to individuals who make requests for their personal information.[77]

f. The Directorates of Human Resources and Defence Health must issue instructions to members of the NZDF authorised to disclose personal information and respond to requests for access to personal information.

g. Unless specifically authorised by the Privacy Commissioner, the NZDF is not permitted to charge for handling information privacy requests.

3.3.2 Disclosure of personal information to ministers

Ministers may have occasion to be provided with or to request personal information held by the NZDF. The Office of the Privacy Commissioner provides a *guide to disclosure of personal information to ministers*, and this should be consulted in the first instance with advice from the NZDF privacy officer as necessary.[78]

3.3.3 Requests for access to personal information may be refused

a. Requests for access to personal information may be refused under the provisions of the PA in certain situations.[79] Conditions may be applied instead of refusing access as detailed in s 54 of the PA.

---

[75] PA, s 4.
[76] PA, s31.
[77] A request may be transferred to another agency. This is considered 'reasonable assistance'.
[78] A copy of the guide is held in the NZDF DDMS Privacy library. The link to the Privacy Commissioner site is *Guidance on disclosure of personal information to Ministers.*
[79] PA, ss 49–53.

b. The NZDF must not refuse access to an individual's personal information, either in part or in totality, without informing the requester of the reasons. A requestor does not need to be advised of NZDF's refusal to provide information to them if doing so may affect an ongoing criminal or judicial investigation, inquiry, national security concerns or the privacy of a third person.[80]

c. Where access to an individual's personal information about themselves is refused, the NZDF has an obligation to advise the requestor of how to contact the Privacy Commissioner in the refusal communication. That person may lodge a complaint with the Privacy Commissioner.[81]

d. Information protected by 'legal privilege' cannot be released or disclosed without the approval of the Attorney-General. Defence Legal Services (DLS) should be consulted if requested information involves legal advice or information connected to litigation.

Section 2 - Compliance

3.3.4 Consequences of non-compliance with the PA

Information is an asset and should be actively protected. The misuse or perceived misuse of personal information erodes public confidence in the government and the NZDF, which may make it harder to collect information in the future. Additionally, other countries may be reluctant to share information with public service agencies if New Zealand does not give proper respect to privacy rights and considerations.

3.3.5 Improper access to personal information

a. A member of the NZDF must not access another individual's personal information unless authorised to do so for proper reasons associated with that individual's role and as necessary for Defence purposes.

b. Improper access to another individual's personal information without sufficient authority is an offence under the *Crimes Act 1961*[82] and, as such, may be referred to the New Zealand Police.

c. A member of the NZDF who improperly accesses another individual's personal information may be subject to disciplinary action under the *Armed Forces Discipline Act 1971* or in accordance with their employment agreement.

[80] PA, s 46(4).
[81] PA, ss 46 and 70.
[82] *Crimes Act 1961*, s 105B.

Section 3 - Sharing of personal information

3.3.6 Sharing personal information within the NZDF

a. The sharing of personal information within the NZDF does not constitute disclosure to a third party and is permitted under the PA. Any internal sharing of personal information must comply with the information privacy principles in the PA and the NZDF policy that personal information should only be shared internally with those who 'need to know'.

b. All members of the NZDF who have access or are granted access to any form of personal information are to protect such information from unauthorised disclosure so far as is practicable. In particular, members of the NZDF must—

(1) ensure that the 'need-to-know' principle is applied in all situations;

(2) ensure that personal information is not left in any area, including workstations, where it can be accessed by people who do not have a need to know;

(3) use secure print functionality when printing personal information; and

(4) only disclose that information where disclosure is necessary to achieve the intended Defence purpose or effect that adheres to the need to know principle.

c. Section 22C of the *Health Act 1956* permits health information about a member of the NZDF to be disclosed to another member of the NZDF for the purposes of administering the provisions of the *Armed Forces Discipline Act 1971* and the *Defence Act 1990*.

3.3.7 Disclosing personal information to a third party

a. The Office of the Chief of Defence Force (OCDF) is the organisational point of contact for information privacy requests.

b. Requests from third parties (whether from individuals, public sector agencies or private sector entities) for personal information about members of the NZDF are requests pursuant to the *Official Information Act 1982* (OIA) and are to be managed by Ministerial Services.

c. If the information is withheld or access refused, the requester must be advised of both the reason/s for refusal as well as their right to lodge a complaint with the Ombudsman.[83]

d. A decision whether to grant a request must be made within 20 working days after the day on which the request is received.

e. Information should be made available in the form requested by the individual unless this would impair efficient administration or be contrary to any legal duty the NZDF may have in respect of the document or information.

[83] OIA, pt 5.

f. Personal information held by the NZDF may be shared with other agencies for the purpose of facilitating provision of public services in accordance with approved information sharing agreements.[84] Examples of disclosure to a third party agency are—

(1) a law enforcement official making a request in the course of an authorised investigation;

(2) a court order or Police obligation to provide evidence in an ongoing trial is presented (does not include medical information);

(3) the non-release of information jeopardising public safety or national security concerns;

(4) the information requested supports the sale of a business or going concern;

(5) a member of Parliament (MP) making a request about a constituent in their electorate; or

(6) other situations where a request is made and considered on a case-by-case basis.

g. If a request for personal information is made by any media representative, the request must be immediately passed to Defence Public Affairs.

3.3.8 Authenticating identity

When ascertaining the identity of a person making a request, a member of the NZDF must be 'reasonably sure' of that person's bona fides. Proof of identity must take the form of either—

(1) a known person;

(2) a picture identification (eg driver licence, identity card or passport); or

(3) a statutory declaration if there is no other means of identification.

3.3.9 Correcting personal information

a. An individual may request that their personal information recorded by the NZDF be corrected.[85]

b. Personal records may be corrected, but, where information is not corrected, the statement requesting the correction is to be added to the personal records in the appropriate place.

c. Corrected information must also be provided to individuals and agencies with whom this information has been disclosed where it is reasonably practicable to do so.

[84] PA, s 139.
[85] PA, ss 22 (information privacy principle 7), 58 and 65.

3.3.10 Sharing personal information with other agencies

a. The government is expected to deliver public services collaboratively. This will often require personal information that has been collected by one agency to be shared with another. The NZDF and public service agencies in receipt of personal information concerning members of the NZDF must employ robust processes for the use and management of personal information.

b. Personal information sharing between agencies must not be conducted without an approved sharing arrangement being authorised in writing by the Chief of Defence Force (CDF) or unless the arrangement is provided for under law by an Act of Parliament or under a legislative instrument.[86]

c. Members of the NZDF must not disclose personal information to another agency for the purposes of 'information matching' without the written permission of CDF.

d. Information about a person may already be held by a public service agency or public body for another purpose. Information can be disclosed to another agency where the disclosure of the information is one of the purposes that the information was obtained or is directly related to the purposes that the information was obtained. Alternatively, it can be shared if disclosure is authorised by the individuals concerned.[87]

e. Ordinarily, information sharing can often be achieved in a way that is consistent with the IPP in the PA. If potential conflicts with the IPP are identified, the information must not be shared. In all cases, appropriate safeguards must be built into information sharing arrangements.

f. Where NZDF elements propose to systemically share personal information held by them, the NZDF must have an approved sharing arrangement authorised by CDF or an approved information sharing agreement made under the PA. The NZDF privacy officer must be consulted. Where doubt exists, the NZDF privacy officer is to seek advice from the Office of the Privacy Commissioner or the Government Chief Privacy Officer (GCPO) before any information is shared with other agencies.

3.3.11 Prohibition on transfer of personal information outside New Zealand

a. Before disclosing the personal information of NZDF members to an overseas entity, the NZDF, including Veterans' Affairs, must believe on reasonable grounds that—

   (1) those overseas entities have similar levels of privacy protection to those in New Zealand;

   (2) that the individual concerned is fully informed and has authorised the disclosure; or

   (3) the disclosure is otherwise authorised under the PA. [88]

[86] The *Veterans' Support Act 2014* is an example of this, as it authorises delegation of powers to the Ministry of Social Development (MSD).
[87] PA, s 22 (information privacy principle 11).
[88] PA, s 22 (information privacy principle 12).

b. The Privacy Commissioner may issue a transfer prohibition notice for a specified country. In all cases of doubt, the NZDF privacy officer is to be consulted.

Section 4 - Reporting privacy issues

3.3.12 Defining a privacy incident

a. A privacy incident occurs when the NZDF does not comply with one or more of the IPP set out in s 22 of the PA (or the applicable code of practice issued under the PA).

b. Privacy incidents are not restricted to unauthorised or accidental access to, or disclosure of, personal information but include breaches of any of the IPP. A breach of a privacy principle may occur without necessarily causing harm to an individual.

c. The NZDF privacy officer is the NZDF authority for determining whether an incident is a near miss or a privacy breach, and whether the Privacy Commissioner needs to be notified. If there is any doubt as to whether there is a privacy issue, the person receiving a report alleging a breach of privacy is to consult the NZDF privacy officer without delay.

3.3.13 Reporting a privacy incident

a. All privacy incidents and near misses are to be reported to the NZDF privacy officer (via the relevant Unit Security Officer (USO) in the first instance, where possible) and are to be initially assessed, contained and, if necessary, as tasked by the NZDF privacy officer, investigated as close to the incident source as appropriate by an appointed individual (normally the USO, privacy champion or delegate). *Annex 3-A* provides a *privacy incident notification template*.

b. The NZDF privacy incident notification template is to be used to identify, categorise and internally report all near misses, breaches of the privacy principles or breaches of NZDF privacy policy. This allows the NZDF to take necessary action in a timely manner, identify systemic organisation trends/issues requiring action and improve system-wide privacy processes accordingly.

c. Any member of the NZDF can raise a privacy issue or suspected privacy incident directly to the NZDF privacy officer if they desire. Such incidents generally involve the disclosure of private information to an unintended audience. Examples include but are not limited to—

(1) documents containing private information being left unsecured on desks or printers;

(2) incorrect distribution or electronic transmission of documents and material comprising private information (eg documents with special handling markings); and

(3) private information in conversations in open-plan areas being overheard.

d. NZDF personnel are to alert the NZDF privacy officer (via their USO in the first instance, where possible) to any privacy issues or suspected privacy incidents immediately using the format in *Annex 3-A* where appropriate. The NZDF privacy officer will determine whether a privacy incident has occurred and will engage with the appropriate commander or manager as appropriate.

e. The NZDF privacy officer is required to report to the Office of the Privacy Commissioner any notifiable breach that it is reasonable to believe has caused serious harm to an affected individual or individuals, or is likely to do so.[89]

f. There are four key steps to be considered when responding to a privacy breach or suspected privacy incident[90]—

(1) Incident containment and preliminary assessment.

(2) Evaluation of the risks associated with the incident.

(3) Notification.

(4) Prevention.

g. Privacy Commissioner Guidelines, as outlined in *Annex 3-B*, are to be used in responding to a privacy incident.[91] In addition, the GCPO has provided a reporting matrix to help identify and report on the scale and severity of a privacy incident (see *Annex 3-C*).[92] This should be used in conjunction with the Privacy Commissioner Guidelines, as it accounts for a broader definition of privacy incident encompassing all the privacy principles beyond access and disclosure incidents.

h. The NZDF also regularly reports to the Foreign Affairs, Defence and Trade select committee on the number and severity of privacy incidents that occur each year. Reporting increases transparency and accountability to the public and to members of the NZDF.

Section 5 - Complaints and privacy investigations

3.3.14 Information privacy complaints

a. The PA provides a comprehensive system for dealing with complaints arising from alleged breaches of the PA. This includes a complaints investigation process administered by the Privacy Commissioner and an appeals process to the Human Rights Review Tribunal. The NZDF maintains an internal process for dealing with privacy incidents and complaints.

[89] PA, pt 6.
[90] The first three steps should be undertaken simultaneously or in quick succession. The final step involves using lessons learned to develop longer-term solutions and prevention strategies. The decision on how to respond is to be made on a case-by-case basis.
[91] These are described in greater detail at *Responding to Privacy Breaches* or the *Privacy Commissioner Data Safety Toolkit*.
[92] Greater explanation of the use of this tool can be found at *Reporting Privacy Breaches*.

b. Any person may make a complaint or complain on behalf of an aggrieved individual(s), concerning an alleged breach of the PA-related legislation or NZDF privacy policies by members of the NZDF. This may be submitted to the individual's commander/manager and the NZDF privacy officer in the first instance. Complaints may also be directed to NZDF persons nominated by name or appointment, specifically—

(1) the NZDF privacy officer;

(2) a Chief of Service (COS) or their delegated representative;

(3) the Commander Joint Forces or their delegate representative;

(4) the Commanding Officer or Senior National Officer of deployed forces; or

(5) a senior NZDF executive or their delegated representative.

c. A complaint alleging a breach of an individual's privacy may be made orally or in writing. An oral complaint must be put in writing by the receiving NZDF commander or manager as soon as practicable.

d. The NZDF privacy officer shall—

(1) investigate, or have investigated, any incident where the provisions of the PA or NZDF privacy policy have, or appear to have, been breached; [93]

(2) keep CDF informed of the progress of investigations and any potential recommendations that may result from the findings of an investigation;

(3) keep the complainant informed of the progress and results of any investigation;

(4) work with Headquarters New Zealand Defence Force (HQNZDF) Ministerial Services and the Privacy Commissioner on any complaint or investigation being dealt with by their office as appropriate; and

(5) take such action as necessary to—

(a) redress the complaint;

(b) advise the person whose personal information has been disclosed of the matter (if not already informed) and any resolution;

(c) advise the Office of the Privacy Commissioner should the incident pose a risk of serious harm;

(d) invoke disciplinary procedures under the *Armed Forces Discipline Act 1971* or the *NZDF Civil Code of Conduct* where appropriate; and

(e) refer a complaint to another official or agency where it is considered that a complaint is more within the jurisdiction of that official or agency.

[93] The NZDF Privacy Office will log the incident, track and review investigations, close or escalate incidents as appropriate.

3.3.15 Investigating privacy incidents and near misses

a. Privacy incidents can range from the low end where there has been a minor breach of a privacy principle, through to a high-end incident that can have potential to cause serious harm.

b. Privacy incidents can be caused by a variety of factors, including complacency, lack of awareness, poor procedures, inadequate security, accidental/inadvertent release or by malicious actions.

c. The NZDF privacy officer will investigate or have investigated any incident where the provisions of the PA or NZDF privacy policy have, or appear to have, been breached as noted. Generally, the privacy officer will personally investigate cases—

(1) that may have implications for NZDF privacy policies;

(2) that may affect the reputation of the NZDF;

(3) that may attract political, media or public interest;

(4) where the Privacy Commissioner may issue an adverse comment;

(5) where results of an investigation may give rise to legal or disciplinary proceedings;

(6) that pose a risk of serious harm;[94] or

(7) that may result in an ex-gratia payment to an individual.

d. It is in the best interests of both individuals and the NZDF for reported incidents to be dealt with at the level and functional area appropriate to the incident, to quickly address issues. COS, heads of portfolio and commanders/managers should proactively address all complaints or potential incidents, keeping the privacy officer updated at all times. Commanders and managers may assess and investigate incidents as long as they are not implicated in the incident.

[94] It is mandatory to report privacy incidents that have caused or are likely to cause serious harm to the Office of the Privacy Commissioner. Affected individuals will need to be notified as soon as possible.

Section 6 - Privacy impact assessment

3.3.16 The need for a privacy impact assessment

a. Introducing a new project or process, or changing existing processes that involve the collection, transfer and storage of personal information, can create privacy risks. These risks can be identified, managed and mitigated by conducting a privacy impact assessment (PIA) early in the consideration process. This assessment can be used to help identify potential risks arising from the collection, use or handling of personal information and to help in informed decision making.[95]

b. A PIA (as for a risk assessment) should be considered alongside other planning considerations for any activity that—

(1) involves personal information about identifiable individuals;

(2) involves information that may be used to identify or target individuals;

(3) may result in surveillance of individuals or intrusions into their personal situation and information; or

(4) may adversely affect an individual's reasonable expectations of privacy.

c. Figure 3-1 provides an initial filter as to whether a PIA may be required. This is covered in more detail in the *Privacy Commissioner Privacy Impact Assessment Toolkit*.[96]

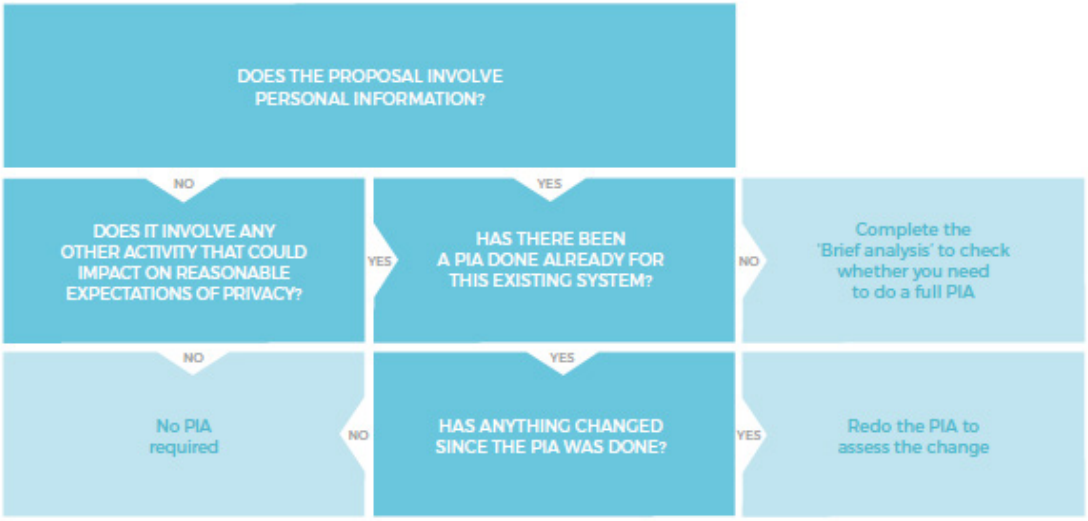

Figure 3-1—Assessment of the need for a PIA.

d. The basic steps in every PIA are—

(1) gather all the information you need to do the PIA and sketch out the information flows;

(2) check against the privacy principles;

(3) identify any real privacy risks and how to mitigate them;

[95] Privacy Commission PIA Toolkit. *Privacy Impact Assessment*.
[96] Also available on the Privacy Commissioner website: *Privacy Impact Assessment Toolkit*

(4) produce a report (use the report template at *Annex 3-D*);

(5) take action; and

(6) review and adjust the PIA as necessary as the project develops.

3.3.17 Conducting a privacy impact assessment

a. It is important to decide whether to do a privacy impact assessment early in any plan or proposal. This is key to the implementation of the privacy by design concept. A failure to identify how a plan, project or proposal is likely to affect personal privacy represents a real risk for the NZDF and for the success of the project/proposal. An example of a new project or activity incorporating a PIA into the planning cycle is represented at Figure 3-2.

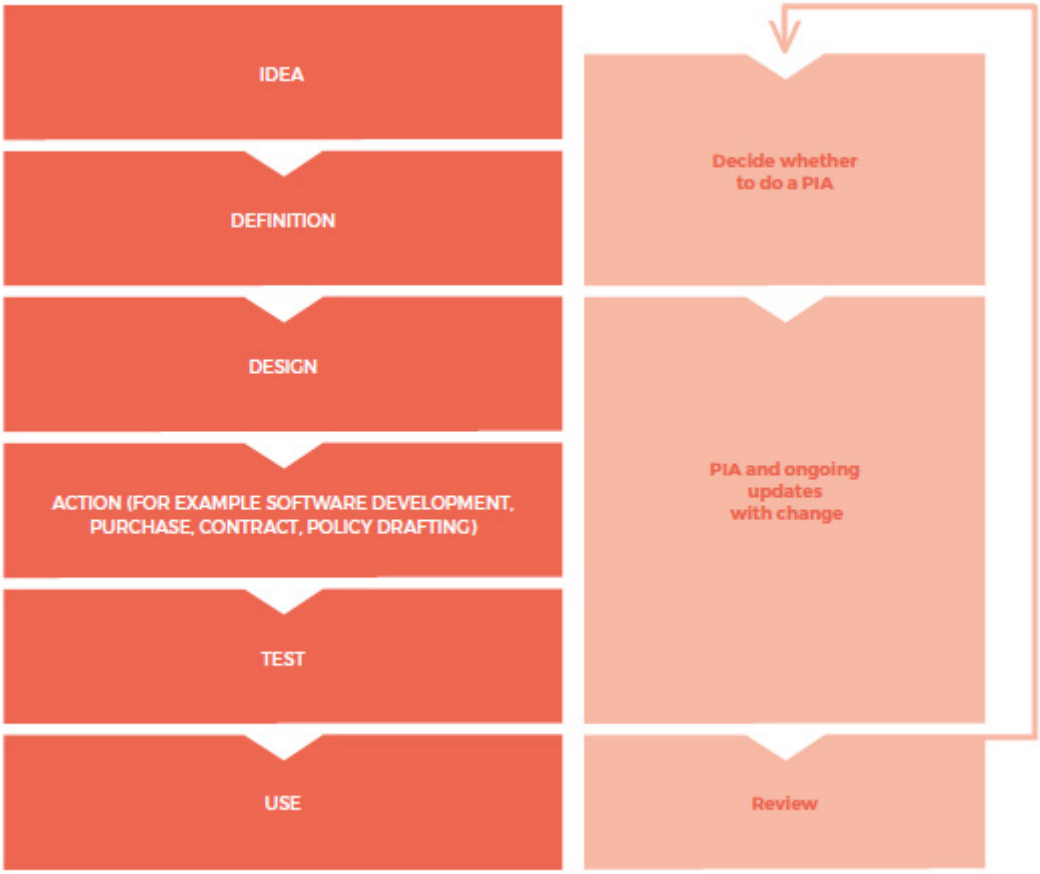

Figure 3-2—Example of a new project/activity incorporating PIA into planning.

b. The privacy impact analysis template at *Annex 3-D* is to be completed for any project or change process where implications for privacy are possible.[97] Use of this tool will provide—

(1) information to inform decision making as to whether a privacy impact assessment is required;

[97] The full treatment of the privacy assessment tool can be found at *Privacy Impact Assessment Toolkit.*

(2) information as to whether the privacy impact assessment is likely to be simple and quick or whether it will be a more complex exercise needing more time and resources; and

(3) a record of the decision-making process in terms of privacy implications.

c. The scale and complexity of a privacy impact assessment will depend on the scale and complexity of the project under consideration and associated risk factors and considerations. A guide and template for conducting a full privacy impact assessment has been produced by the *Privacy Commissioner* and is to be followed where a full assessment is required.[98]

d. In all cases where personal information is collected and managed a Privacy Statement should be used to advise what information is being collected, for what purpose and how it is being protected.

e. The Privacy Commission has a *Privacy Statement Generator Tool*. The NZDF Privacy Officer can provide advice on Privacy Statements and is to review and approve these statements.

Annexes to Chapter 3

[98] A privacy impact assessment guide is available at *Part 2: How to do a Privacy Impact Assessment (PIA)*. *This is supported by a Privacy Impact Assessment Report and a Risk and Mitigation Table.*

ANNEX 3-A

PRIVACY INCIDENT/NEAR MISS INCIDENT NOTIFICATION TEMPLATE

1. A privacy incident can occur for a range of reasons, and when this happens, it is important that everything is done to minimise the harm they may cause.

2. When a privacy issue has been identified, whether an incident, suspected incident or a near miss, the NZDF privacy officer must be provided with the following information without undue delay—

Table 1—Privacy incident/near miss notification template

(Date)	**PRIVACY INCIDENT/NEAR MISS INCIDENT NOTIFICATION**	Remarks
Point of Contact	Name and contact details	
Date and time of incident		
What	Describe the privacy incident or near miss. Keep this statement factual and concise.	
Who	Who is impacted (or potentially impacted) by this?	
When	When did this occur? Is it ongoing or has it been stopped?	
Where	Where did the incident occur?	
How	If known what was the cause of the incident or near miss?	

3. If appropriate, complete the Privacy Incident Reporting Matrix at *Annex 3-C* by marking the statements that best fit the present situation.

ANNEX 3-B

GUIDELINES FOR RESPONDING TO A PRIVACY INCIDENT

1. A privacy incident can occur for a range of reasons and, when this happens, it is important that everything is done to minimise the harm that it might cause.

Key steps in responding to a privacy incident[99]

2. There are four key steps in dealing with a privacy incident—
   a. Step 1: Contain.
   b. Step 2: Assess.
   c. Step 3: Notify.
   d. Step 4: Prevent.
3. Move quickly to investigate the suspected incident and its potential for harm. Consider the potential for harm to the individuals to whom the incident relates, harm to the public's trust in the NZDF and harm to its reputation.
4. Steps 1–3 should be undertaken either simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and incident prevention strategies. The decision on how to respond should be made on a case-by-case basis.
5. Factors that need to be considered—
   a. What is the risk of harm to people whose information has been breached?
   b. Is there a risk of identity theft or fraud?
   c. Is there a risk of physical harm?
   d. Is there a risk of humiliation or loss of dignity, damage to the individual's reputation or relationships, eg when the information lost includes mental health, medical or disciplinary records?
   e. What is the person's ability to avoid or minimise possible harm?
   f. What are the legal and contractual obligations?

Step 1: Contain

6. Once you have discovered that a potential incident has occurred, you should quickly take common sense steps to limit any damage—
   a. **Immediately contain the incident**. For example, while you diagnose what went wrong, stop the practice that allowed the incident, try and get back the records, consider disabling the system that was breached, cancel or change the computer access codes and try to fix any weaknesses in physical or electronic security.
   b. **Find a suitable person to lead the initial assessment or investigation**. This person should be in a position to carry out the initial assessment or investigation and make the first recommendations. A more detailed investigation/review can be carried out later.

[99] *Responding to Privacy Breaches*.

c. **Decide whether to put a team together that could include people from other areas**. This might include people from within the NZDF or subject matter experts from outside who have the expertise to deal with the situation (eg IT analysts or risk advisers).

d. **Decide who needs to be informed**. Build up a list of those who need to be told. The NZDF privacy officer is the primary point of contact. Consider other parties who may need to be informed, such as NZDF insurance advisors, NZDF Audit and DLS.

e. The NZDF privacy officer will notify the New Zealand Police if the incident appears to involve theft or other criminal activity (and seek appropriate approval for this course of action).

f. The NZDF privacy officer will notify the Privacy Commissioner if the incident is assessed as having caused (or being likely to cause) serious harm.

g. Do not compromise your ability or the ability of investigators to investigate the incident. Be careful not to destroy evidence that may be valuable in finding the cause of the problem or that might allow you to fix the issue.

Step 2: Assess

7. To determine what other steps are needed, you need to assess the risks caused by the incident. An evaluation of the type of information involved will help you determine how to respond to the incident, who should be informed (including potentially the Office of the Privacy Commissioner) and also whether it is appropriate to tell the individuals affected. There are a number of factors to consider—

   a. **What kind of personal information is involved?** The more sensitive the information, the higher the risk of harm to the people affected. Health information, date of birth, driver licence numbers and credit card details can all cause harm on their own but if used together, could be used for identity theft. A combination of personal information is typically more sensitive than a single piece of personal information.

   b. **Is the personal information easy to get at?** If the information is not password secured or encrypted, then there is a more real risk of it being misused.

   c. **What caused the incident?** Try and find out what caused the incident and if there is a risk of further incidents or further exposure of the information.

   d. **What is the extent of the incident?** Try and identify the size of the incident, including the number and nature of the likely recipients as well as how many people's personal information has been lost/disclosed. It is also important to identify the risk of the information being circulated further. Find out if the incident is the result of a systemic problem or an isolated incident.

   e. **Assess whether harm could result from the incident.** Consider this from the point of view of the people affected. Types of harm could include identity theft, financial loss, loss of business or employment opportunities, significant humiliation or loss of dignity. Assess the harm to the NZDF, eg loss of trust and

reputation damage, financial exposure or legal proceedings. What steps have already been taken to mitigate the harm?

f. **Is the information in the hands of people whose intentions are unknown or possibly malicious?** Eg was the information taken by, or given to, an unknown recipient or one suspected of illegal activity? Was the recipient a trusted, known person or organisation that could be expected to return the information?

8. The Privacy Incident Reporting Matrix at *Annex 3-D* can be used to assess the scale and severity of the privacy incident.

Step 3: Notify

9. Being open and transparent with individuals about how personal information is being handled is a fundamental rule of privacy. Notification can be a key step in helping individuals affected by the incident and showing the NZDF is doing the right thing. If a data incident creates a risk of serious harm to the individual, those affected must be notified. Prompt notification can help them lessen the damage by taking steps to protect themselves and regain control of that information. The Privacy Commissioner must also be notified when there is a risk of serious harm. In all cases, guidance from the NZDF privacy officer is to be sought before any notification to affected people or the matter is escalated to the Privacy Commissioner.

10. Do not notify people unless you are sure of the people whose information has been compromised by the incident. More damage can be done if the wrong people are notified in error.

11. If there is no risk of harm, notification can be unnecessary and, on occasion, can do more harm than good. Each incident needs to be considered on a case-by-case basis.

Notification

12. At this stage, you should have as complete a set of facts as possible and have completed a privacy incident impact assessment in order to determine whether to notify individuals. Notification should occur as soon as reasonably possible. If law enforcement authorities are involved, check with those authorities on when to notify so that their investigation is not compromised.

13. **How to notify.** It is always best to notify affected individuals directly – by phone, letter, email or in person. Direct notification is more sincere and personal. Indirect notification (website information, posted notices, media etc) should generally only occur where direct notification could cause further harm, is prohibitively costly or the contact information is not known. Using multiple methods of notification may also be appropriate. It is also important to consider whether notification might reveal the value of the missing information. For particularly vulnerable people, you might need to consider notifying them through or with a support person where sensitivity and discretion is required.

14. **Who should notify?** The immediate commander or manager who has a direct relationship with the subject of the incident should be the party to notify the affected people. For example, if 'Staff-in-Confidence' information is accidentally emailed to another NZDF member, the immediate commander/manager should advise the subject

of the incident as soon as practicable. As noted in *3-21*, consultation with the privacy officer is required before notification.

15. **What should be included in a notification?** Incident notifications should generally contain—

    a. information about the incident, including when it happened;

    b. a description of the personal information that has been disclosed and what has not been disclosed;

    c. what the Service or Portfolio is doing to control or reduce the harm;

    d. what it is doing to help people and what steps they can take to protect themselves;

    e. contact information for enquiries and complaints;

    f. offers of assistance when necessary, eg advice on changing passwords;

    g. whether it is recommended to notify the Office of the Privacy Commissioner;[100] and

    h. contact information for the Privacy Commissioner, as applicable.

16. **Notifying third parties**. Bearing in mind any obligations of confidentiality, consider whether the following groups or organisations should also be informed—

    a. The New Zealand Police (if theft or other crime is suspected).

    b. Insurers (if required by contractual obligations).

    c. Professional or other regulatory bodies (if professional or regulatory standards require notification of these bodies).

    d. Credit card companies, financial institutions or credit reporting agencies (if their assistance is necessary for contacting individuals or assisting with mitigating harm).

    e. Third party contractors or other parties who may be affected.

    f. Internal business units not previously advised of the privacy incident, eg government relations, communications and media relations, or other members of senior management.

    g. The Government minister.

    h. The relevant union or other employee representatives.

17. The Office of the Privacy Commissioner must be notified of any incident where there is a risk of serious harm. Such notification is to be through the NZDF privacy officer. This will provide awareness and help the Privacy Commissioner to better handle any related enquiries or complaints. The Privacy Commissioner may also be able to provide advice or guidance to the NZDF that may be helpful in responding to the incident.

[100] Note the mandatory requirements for incident reporting related to serious harm.

Step 4: Prevent

18. Do not assume that there is nothing that can be fixed or done to prevent future mistakes. There is a system failure behind many errors, and the present incident provides an opportunity to learn from the causes. There are a number of steps the NZDF can take to minimise or prevent privacy incidents. The most effective is having a well-thought-out security plan for all personal information.

19. In the aftermath of a privacy incident, the NZDF should review its privacy policies. Assessments, investigations and reviews within the NZDF as a result of a privacy incident must note the cause of the incident and make changes as required to prevent a repeat.

20. The amount of effort should reflect the significance of the incident and whether it happened as a result of a systemic problem or an isolated event. It could include—

    a. a security audit of both physical and technical security;

    b. a review of policies and procedures;

    c. a review of employee training practices; or

    d. a review of any service delivery partners caught up in the incident.

21. The resulting prevention plan may include a requirement for an audit to ensure that the plan has been fully embedded into the organisation.

ANNEX 3-C

REPORTING MATRIX FOR IDENTIFYING THE SCALE AND SEVERITY OF A PRIVACY INCIDENT

1. The following matrix was developed by the GCPO to provide a tool to identify and report on the scale and severity of privacy incidents and near misses.[101] It may also assist in providing context around privacy incidents and near misses reported internally or to the public through official documents such as annual reports. The matrix is to be used by the NZDF for this purpose.

Using the matrix

2. The matrix has seven key areas to be assessed—
   a. Number of individuals affected.
   b. Sensitivity of the information at issue.
   c. Harm to the individual.
   d. Harm to the agency.
   e. Potential for media attention.
   f. Source of the privacy incident.
   g. Whether the information has been recovered, accessed or able to be accessed.
3. Each assessment response is assigned a value, the total of which determines the rating of the privacy incident. The purpose of the ratings is to provide an indication of the severity and scale of the privacy incident. The ratings are a blunt tool and may not fit every single privacy incident, but they enable uniform reporting. If the specific characteristic of a privacy incident warrants it, the event can be placed in a higher graded level. At all times, the impact of public reporting on the individual(s) concerned must be paramount.

Reporting privacy incidents

4. The GCPO suggests agencies regularly report information about privacy incidents and near misses externally (eg in the annual report or on the agency website) and suggests the following criteria—
   a. Privacy incidents and near misses that fall within levels 1 and 2 may not be appropriate to report externally.
   b. Privacy incidents and near misses that fall within level 3 may be reported.
   c. Privacy incidents and near misses that fall within levels 4 and 5 should be reported.
5. It is important that only privacy incidents that meet a certain threshold are reported. When considering whether a privacy incident or near miss should be reported externally, there needs to be assurance that this release does not involve any inadvertent further harm to any individual.

[101] GCPO terminology is shifting away from 'breaches' to 'incidents'. An incident can include a breach or a near miss.

6. Privacy incidents that fall within levels 1 and 2 may also be reported where several privacy incidents of a similar type or from a similar source helped identify a systemic problem.

7. Where an incident relates to unauthorised or accidental access to or disclosure of personal information and there is a risk of serious harm, the incident must be reported to the Privacy Commissioner and to the parties involved through the NZDF process as described earlier – refer to Part 3, Chapter 3, Section 4.

Table 1—Privacy incident reporting matrix

Criteria	Detail	Rating
Number of individuals affected	Single individual	10
	2–10 individuals	20
	11–50 individuals	40
	51 or more individuals	60
Sensitivity of the information (Select the highest level of sensitivity involved)	Minor sensitivity (eg name, employment position)	10
	More sensitivity (eg remuneration, contact details)	20
	Sensitive (eg financial, biometric)	50
	Highly sensitive (eg health, criminal records, information about people at risk, closed records, contact details for vulnerable people)	80
Potential or actual harm to the individual(s) (You can select several types of harm potential and/or actual harm. If actual harm occurred, do not select the corresponding potential harm)	No potential or actual harm to the individual(s)	0
	Potential for financial loss to the individual(s)	20
	Actual unwanted intrusion into the individual's personal life	20
	Potential for identity theft	25
	Potential for loss of business, employment or other opportunities for the individual(s)	25
	Potential for hurt, humiliation or reputational damage to the individual(s)	30
	Individual denied access to/correction of or statement of correction not included with their information without good reason	30
	Actual financial loss to the individual(s)	40
	Potential for physical harm to the individual(s)	50
	Actual identity theft	50
	Actual loss of business, employment or other opportunities for the individual(s)	50
	Actual hurt, humiliation or reputational damage to the individual(s)	60
	Actual physical harm to the individual(s)	100
Potential or actual harm to the agency (If several types of potential and/or actual harm are relevant, select 'More than one type	No potential or actual harm to the agency	0
	Potential for loss of business opportunity for the agency	10
	Potential for financial loss to the agency	20
	Potential for reputational damage to the agency	20
	Potential for loss of trust in the agency or wider public sector	20
	Loss of business opportunity for the agency	20
	Financial loss to the agency	40
	Reputational damage to the agency	40
	Loss of trust in the agency or wider public sector	40

Table 1—Privacy incident reporting matrix

Criteria	Detail	Rating
of harm to the agency').	More than one type of harm to the agency	50

Criteria	Detail	Rating
Potential for media attention	No media interest occurring or likely to occur	0
	Some media interest occurring or likely to occur	20
	Widespread media interest occurring or likely to occur, and the agency, GCPO, Office of the Privacy Commissioner (OPC) and others	50
Privacy incident source	Inadvertent information handling error (eg email or letter sent to incorrect recipient, or information provided to the wrong person over the telephone)	10
	Information used by the agency for a purpose not related to collection, and an exception does not apply	20
	Failure to provide access to personal information within statutory or extended timeframe, or failure to correct or attach a statement of correction to personal information	30
	Theft or loss of property containing personal information (eg USB stick, documents)	40
	Information collected by unlawful, unfair or unreasonably intrusive means	50
	Unauthorised access of systems or information (eg staff member accessing information not for work purposes and contrary to agency policies/procedures)	50
	Systemic system or business process issue (eg insufficient security controls, asking for and receiving information not necessary for purpose, not responding to requests, withholding information without good reason or retaining information received through an information-matching programme)	60
	Cyber security incident (eg hacking)	60
Status of the privacy incident	Information recovered/destroyed and not accessed by an unauthorised individual	1
	Individual provided access to their information, or information corrected/statement of correction included	10
	Information not recovered but encrypted and unlikely to be accessible	20
	Information recovered/destroyed/no physical copy disclosed and accessed by an unauthorised individual(s)	50
	Systemic or business process issue fixed, but information was accessed by an unauthorised individual(s)	50
	Information not recovered and accessible	60

Table 2—Privacy incident impact ratings

Rating range	Level	Descriptor
0–170	1	Small number of people affected, with little or no potential or actual harm to the individual(s). Little or no indication of systemic problems within the agency. Agencies should consider tracking these privacy incidents and taking corrective action if there are a number from a similar source.
171–220	2	Small number of people affected, with minor potential or actual harm to the individual(s). Little or no indication of systemic problems within the agency. Agencies should consider tracking these privacy incident and taking corrective action if there are a number from a similar source.
221–270	3	Either the information is not sensitive/highly sensitive and the potential or actual harm to the individual(s) is more than minor; or the information is sensitive/highly sensitive and the potential or actual harm to the individual(s) is minor. Customers may stop using, or be reluctant to use, a service or delivery channel. The incident may get media attention or cause reputational risk.
271–320	4	Incident of sensitive or highly sensitive information, with serious potential or actual harm to the individual(s). The incident may imply a systemic failure that could undermine agency systems. The incident may cause long term loss of trust and confidence in the agency that could impact service delivery. There could be measurable and ongoing negative impact on individuals and/or agencies. Ongoing media coverage.
321 and above	5	Incident of sensitive or highly sensitive information, with serious potential or actual harm to the individual(s). It is likely that more than one type of harm has occurred, and that harm is likely to be ongoing. There may be a systemic failure that could undermine agency systems. If public, will significantly affect the reputation of and trust and confidence in the state sector. Ongoing media coverage.

ANNEX 3-D

PRIVACY IMPACT ANALYSIS TEMPLATE[102]

BRIEF PRIVACY IMPACT ANALYSIS REPORT: [PROJECT/PROPOSAL NAME]

Project summary: [Project/proposal name]

1. **Brief description of the project—**
   a. Describe the existing systems and the key changes that are proposed.
   b. Describe the purpose of the change or development of the proposal, including key benefits to the NZDF or to affected individuals.
   c. Identify the main stakeholders or entities involved and their role in the project/proposal.

2. **Personal information involved.** Table 1 of *Annex 3-C* describes—
   a. the personal information that will be collected, used, and/or disclosed;[103]
   b. the source of the information; and
   c. the purpose of the information.

Table 1—Personal information involved

Type of personal information	Source of information	Purpose of information for the project

Privacy assessment

3. **Areas that are risky for privacy.** Some types of projects are commonly known to create privacy risks. If the project involves one or more of the risk areas outlined in Table 2, it's likely that a PIA will be valuable.

[102] A Word version of this template is available at *Privacy Impact Analysis Template*.
[103] 'Personal information' is any information about an identifiable living person. However, a person does not have to be named in the information to be identifiable.

Table 2—Privacy risk checklist

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Information management generally			
A substantial change to an existing policy, process or system that involves personal information ***Example**: New legislation or policy that makes it compulsory to collect or disclose information*			
Any practice or activity that is listed on an NZDF risk register ***Example:** Practices or activities listed on your unit's/portfolio's privacy risk register or health and safety register*			
Collection			
A new collection of personal information ***Example:** Collecting information about individuals' location*			
A new way of collecting personal information ***Example:** Collecting information online rather than on paper forms*			
Storage, security and retention			
A change in the way personal information is stored or secured ***Example:** Storing information in the cloud*			
A change to how sensitive information is managed ***Example:** Moving health or financial records to a new database*			
Transferring personal information offshore or using a third-party contractor ***Example:** Outsourcing the payroll function or storing information in the cloud*			
A decision to keep personal information for longer than you have previously ***Example:** Changing IT backups to be kept for 10 years when you previously only stored them for 7*			
Use or disclosure			
A new use or disclosure of personal information that is already held ***Example:** Sharing information with other parties in a new way*			
Sharing or matching personal information held by different organisations or currently held in different datasets ***Example:** Combining information with other information held on public registers, or sharing information to enable organisations to provide services jointly*			

Table 2—Privacy risk checklist

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Individuals' access to their information			
A change in policy that results in people having less access to information that you hold about them ***Example:*** *Archiving documents after 6 months into a facility from which they can't be easily retrieved*			
Identifying individuals			
Establishing a new way of identifying individuals ***Example:*** *A unique identifier, a biometric, or an online identity system*			
New intrusions on individuals' property, person or activities			
Introducing a new system for searching individuals' property, persons or premises ***Example:*** *A phone company adopts a new policy of searching data in old phones that are handed in*			
Surveillance, tracking or monitoring of movements, behaviour or communications ***Example:*** *Installing a new CCTV system*			
Changes to your premises that will involve private spaces where clients or customers may disclose their personal information ***Example:*** *Changing the location of the reception desk, where people may discuss personal details*			
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them ***Example:*** *Adding a new medical condition to the requirements of a pilot's license*			
List anything else that may impact on privacy, such as bodily searches or intrusions into physical space			

4. **Initial risk assessment.** Table 3 provides the initial risk assessment for each aspect of the project based on the findings from the checklist at Table 2.

[If you answered "Yes" to any of the questions in Table 2, use Table 3 to give a rating – either low (L), medium (M), or high (H) – for each of the aspects of the project set out in the first column.

For risks that you've identified as 'medium' or 'high', indicate (in the right-hand column) how the project plans to lessen the risk (if this is known).

If you answered "No" to all the questions move on to the next section.]

Table 3—Initial risk assessment

Aspect of the project	Rating (L, M or H)	Describe any medium and high risks and how to mitigate them
Level of information handling L – Minimal personal information will be handled M – A moderate amount of personal information (or information that could become personal information) will be handled H – A significant amount of personal information (or information that could become personal information) will be handled		
Sensitivity of the information (eg health, financial, race) L – The information will not be sensitive M – The information may be considered to be sensitive H – The information will be highly sensitive		
Significance of the changes L – Only minor change to existing functions/activities M – Substantial change to existing functions/activities; or a new initiative H – Major overhaul of existing functions/activities; or a new initiative that's significantly different		
Interaction with others L – No interaction with other agencies M – Interaction with one or two other agencies H – Extensive cross-agency (government) interaction or cross-sectional (non-government and government) interaction		
Public impact L – Minimal impact on the NZDF and stakeholders M – Some impact on stakeholders is likely due to changes to the handling of personal information; or the changes may raise public concern H – High impact on stakeholders and the wider public, and concerns over aspects of project; or negative media is likely		

Summary of the privacy impact

5. Table 4 provides a summary of the assessed privacy impact.

Table 4—Assessed privacy impact

The privacy impact for this project has been assessed as:	Tick
Low – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated	
Medium – Some personal information is involved, but any risks can be mitigated satisfactorily	
High – Sensitive personal information is involved, and several medium to high risks have been identified	
Reduced risk – The project will lessen existing privacy risks	
Inadequate information – More information and analysis is needed to fully assess the privacy impact of the project	

6. **Reasons for privacy impact rating.**

(Briefly summarise your reasons for the assessed impact rating.)

Recommendation

7. **Do a full privacy impact assessment.**

Describe—

- the likely timing of the PIA;
- the level of complexity that will be needed; and
- who will be responsible for doing the PIA.

or

8. **A full privacy impact assessment is not required.**

- Explain why a PIA is not needed.

[NAME]
[RANK]
[Position]

End Matter

Record of Change

Amendment Number	Commencement Date	Reference	Details of Change	Approving Authority
V1.00	11 Dec 20	70121696	Initial Issue Supersedes DFO 70. All previous orders, directions and instructions for managing the access to official information in the NZDF have been repealed.	**AJ WOODS** Air Commodore Chief of Staff HQNZDF

Note: Record of Change terminology—

On Issue Initial issue or subsequent reissue of the publication.

Withdrawn A complete publication is withdrawn for use by the NZDF.

Repealed A complete part of a Defence Force Order or Defence Force instruction is repealed/cancelled.

Replaced Complete parts, chapters or sections may be replaced with new parts, chapters or sections.

Inserted New text may be inserted within parts, chapters or sections.

Substitute Published text is substituted with new text or words.