



19 September 2023



Ref: OIA-2023/24-0160

Dear

Official Information Act request relating to the handling of OIA requests related to COVID-19 vaccinations

Thank you for your Official Information Act 1982 (the Act) request received on 29 August 2023. You requested:

“Dear Department of the Prime Minister and Cabinet, Please would you share all the correspondence on policies, procedures, memos etc relating to the process and handling of official responses to Official Information Act requests relating to any Covid-19 vaccination matters.

*This request is for the timeframe of Jan 2021 until Sept 2022.
I am requesting all correspondence on policy, procedures, memos etc relating to the subject of Covid-19 vaccination for handling of any OIA for the above date range.”*

The Department of the Prime Minister and Cabinet (DPMC) handles all Official Information Act (OIA) requests in the same manner regardless of the subject. I am therefore refusing your request for *correspondence on policies, procedures, memos etc relating to the process and handling of official responses to Official Information Act requests relating to any Covid-19 vaccination matters for the timeframe of Jan 2021 until Sept 2022* under section 18(e) as the information requested does not exist.

I can however provide you with the following information regarding DPMC’s handling of OIA requests.

DPMC has a centralised Ministerial Services Team that oversees the administration of, and provides advice to DPMC business units on, responding to OIA requests. The Ministerial Services team also supports the National Emergency Management Agency (NEMA), which is a Departmental Agency hosted by DPMC. The policies and procedures for responding to Official Information Act requests apply to both DPMC and NEMA.

Please find attached the following documentation setting out DPMC’s policy and procedures for processing of requests:

Document	Description	Decision
Document 1	DPMC and NEMA Official Information Act Quick Guide	Release in full
Document 2	DPMC and NEMA Intranet (Kainga) page on Official Information Act Guide for DPMC and NEMA staff.	Email address withheld under section 9(2)(g)(ii).
Document 3	DPMC and NEMA Guide on working with the Ministerial Services team on Official Information Act requests.	Release in full
Document 4	Ministerial Services Triage Considerations.	Release in full

Document	Description	Decision
Document 5	Ministerial Services Quality Assurance Checklist	Release parts relating to OIA responses in full
Document 6	Release of staff personal information under the Official Information Act.	Release in full

The documents provided here are the most relevant, setting out DPMC's policies and procedures for responding to requests under the Act for all of DPMC and NEMA. Please note that individual business units may have internal processes that they follow when engaging with the Ministerial Services Team on responding to requests.

DPMC uses the guidance for agencies responding to OIA requests available from both the Office of the Ombudsman and Te Kawa Mataaho Public Service Commission (PSC). The documents provided do not have specific review dates but are reviewed and revised regularly and if necessary amended to reflect the latest guidance from the Ombudsman and PSC. This ensures that our processes are in line with best practice. Amendments are also needed when DPMC business units close or new business units are established.

In November 2022 DPMC began a review of its processes for responding to Official Information Act requests which has just been completed. The process map for OIA requests developed through this review is yet to be finalised and rolled out across DPMC. Accordingly, this is not in use by DPMC at this time and for that reason is considered out of scope of your request and has not been included in our response.

In making my decision, I have considered the public interest considerations in section 9(1) of the Act. No public interest has been identified that would be sufficient to override the reasons for withholding that information.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on the Department of the Prime Minister and Cabinet's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely



Clare Ward
Executive Director
Strategy, Governance and Engagement

What information does the OIA cover? Section 2(1)

Any information held by a department, an organisation, or a Minister of the Crown in their official capacity. Its more than just documents, it also includes...oral advice, telephone conversations, discussions in meetings, and text messages

THE OIA DOES NOT REQUIRE A MINISTER, OR OFFICIALS TO FORM AN OPINION, AS THIS IS NOT OFFICIAL INFORMATION
(e.g. Will the Minister be supporting the proposal from DPMC?)

Who can make an OIA request? Section 12(1)

Any person being a – NZ citizen, a permanent resident, a person who is in NZ. Body corporates can also make requests as long as they are incorporated in NZ or have a place of business in NZ

How long do I have to respond? Section 15A

The department has to respond to the requestor 'as soon as reasonably practicable' and no later than **20 working days** after receipt

What constitutes a response?

Within the 20 working days, the department is obliged to provide either:

- ❖ a decision on request, and/or
- ❖ Extend the time to respond within 20 working days, and/or
- ❖ Transfer the request to another department (within 10 days unless extended)

How can eligible people make requests? Section 12 (1AA)

- ❖ Requests do not need to be made in writing (e.g. they can be made over the phone or in person)
- ❖ Requests do not need to be made in any particular format so things such as **t** and **f** messages count as OIA requests
- ❖ Requests do not have to cite the OIA
- ❖ The requestor does not need to give a reason for wanting the information

However...for the request to be valid, it must have...

Due particularity Section 12(2)

The Ombudsman defines due particularity as the request being "specific enough to enable the information sought to be readily identified"

If the request is too vague and does not meet the test for due particularity, then...

- ❖ The department has an obligation to assist the requestor to refine the request (Section 13)
- ❖ If the requestor cannot (or will not) refine the request, the department can consider refusing the request under Section 18

What do I do if there is information that is sensitive and not suitable for release?

The OIA contains provisions for withholding information

(a further description of section 6 & 9 withholding grounds are on the reverse of this sheet)

Withholding and refusal sections

Section 6

These are **conclusive** reasons to withhold information therefore, once you have decided that this applies, the information is withheld automatically and is **NOT** subject to a public interest test

Section 9

These are reasons for withholding information that are subject to a **public interest test**. So you need to ask yourself, does the reason to withhold the information outweigh the public interest?

Can I refuse a request for administrative reasons? Section 18

Sometimes there are administrative reasons for withholding which are not subject to a public interest test. This is when information cannot be released for practical reasons. You can withhold if releasing the information is; in contempt of the house, publically available, available under the Criminal Disclosure Act, the information does not exist or, cannot be made available without substantial collation and research

QUESTIONS? NEED HELP?

Contact Ministerial Services:
Information@dpmc.govt.nz

Section 6 and 9 withholding grounds

Section 6 and 9 of the OIA contain most of the commonly used withholding grounds and is a good place to start when considering information under the OIA. You can find the full legislation online at www.legislation.govt.nz

Section 6 - Good reason for withholding official information exists under Section 6 if the making available of that information would be likely—

- (a) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or
- (b) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by—
 - (i) The Government of any other country or agency of such a Government; or
 - (ii) Any international organisation; or
- (c) to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; or
- (d) to endanger the safety of any person; or
- (e) to damage seriously the economy of New Zealand by disclosing prematurely decisions to change or continue government economic or financial policies.

Section 9(2) - This section applies if, and only if, the withholding of the information is necessary to—

- (a) protect the privacy of natural persons, including that of deceased natural persons
- (b) protect information where the making available of the information—
 - (i) would disclose a trade secret; or
 - (ii) would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information
- (ba) protect information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information—
 - (i) would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied; or
 - (ii) would be likely otherwise to damage the public interest;
- (c) avoid prejudice to measures protecting the health or safety of members of the public; or
- (d) avoid prejudice to the substantial economic interests of New Zealand; or
- (e) avoid prejudice to measures that prevent or mitigate material loss to members of the public; or
- (f) maintain the constitutional conventions for the time being which protect—
 - (i) the confidentiality of communications by or with the Sovereign or her representative;
 - (ii) collective and individual ministerial responsibility;
 - (iii) the political neutrality of officials;
 - (iv) the confidentiality of advice tendered by Ministers of the Crown and officials; or
- (g) maintain the effective conduct of public affairs through—
 - (i) the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any department or organisation in the course of their duty;
 - (ii) the protection of such Ministers, members of organisations, officers, and employees from improper pressure or harassment; or
- (h) maintain legal professional privilege; or
- (i) enable a Minister of the Crown or any department or organisation holding the information to carry out, without prejudice or disadvantage, commercial activities; or
- (j) enable a Minister of the Crown or any department or organisation holding the information to carry on, without prejudice or disadvantage, negotiations (including commercial and industrial negotiations); or
- (k) prevent the disclosure or use of official information for improper gain or improper advantage.

Official Information Act (OIA) Requests

What is the Official Information (OIA) Act 1982?

Owner: Amy Teague [DPMC] (<https://kainga/help-n>)
 Team: Ministerial Services
 Email: [S9\(2\)\(g\)\(ii\)@dpmc.govt.nz](mailto:S9(2)(g)(ii)@dpmc.govt.nz)
 Modified: 23/05/2023

The OIA is legislation which forms part of New Zealand's constitutional framework and gives New Zealanders the right to access information held by the government. It supports public participation in government and is designed to increase accountability and transparency.

The OIA is based on the principle of availability which means that "information shall be made available unless there is good reason for withholding it."

Our OIA Quick Guide outlines the basics: [📄 Official Information Act-Quick Guide-.pdf \(/help-me-with/PublishingImages/Pages/OIA-requests/Official%20Information%20Act-Quick%20Guide-.pdf\)](#)

Frequently Asked Questions

Can I withhold my name and contact details under the OIA?

The Ombudsman recently released guidance relating to the withholding of public sector staff names and contact details. In summary the Ombudsman view is that:

"The names of officials should, in principle, be made available when requested. All such information normally discloses is the fact of an individual's employment and what they are doing in that role. Anonymity may be justified if a real likelihood of harm can be identified but it is normally reserved for special circumstances such as where safety concerns arise".

Here is the full guidance: [📄 Names and contact details of public sector employees.pdf \(/help-me-with/PublishingImages/Pages/OIA-requests/Names%20and%20contact%20details%20of%20public%20sector%20employees.pdf\)](#)

With a few exceptions (mostly in PAG and NSG) the approach DPMC takes aligns with this guidance and we assess the need to withhold names and contact details on a case-by-case basis. To help establish when a name (or the associated contact details) need to be withheld, the Ombudsman has produced a useful worksheet:

[📄 Work sheet for processing requests for names of public sector employees.pdf \(/help-me-with/PublishingImages/Pages/OIA-requests/Work%20sheet%20for%20processing%20requests%20for%20names%20of%20public%20sector%20employees.pdf\)](#)

If you have any questions, or would like to know more, the Ministerial Services team are happy to help, just send us an email: information@dpmc.govt.nz (mailto:information@dpmc.govt.nz)

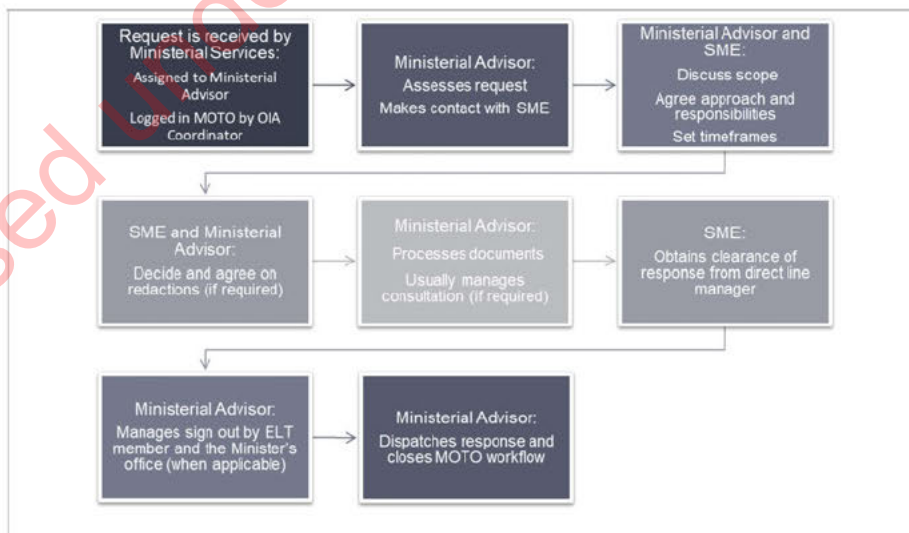
Processing OIA requests at DPMC

Sometimes the amount of OIA requests, correspondence, and Written Parliamentary Question(WPQ) work puts additional strain on the capacity of the business group. This often happens when the business group is already busy however, it is important that Subject Matter Experts (SMEs) and business group managers are involved in the decision-making and approval of the release of their own information.

To support DPMC business groups to meet their obligations, Ministerial Services provides;

- administrative support,
- manages processes and timelines, and
- provides any other reasonable requests for support that is required to progress ministerial work.

High-level process for OIA requests:



Best Practice timelines

Day 1	Request received in the information@dpmc.govt.nz mailbox
By day 2	Acknowledged by coordinator (via MOTO) and allocated to advisor by manager
By day 3	Initial assessment of request by advisor completed including, proposed timelines and actions to be taken. Email sent to business unit.

By day 5	Scope discussed with business unit, approach and responsibilities are agreed, timeframes confirmed.
By day 7	If required, re-scoping email sent to requestor.
By day 10	Documents reviewed and/or processed. Decision made on transfer of requests and preliminary decisions made on need to consult/extend request (if requested is to be extended, new timeline and due dates are sent to relevant people).
Between day 10-15	QA and sign out process commences
By day 15	MOIAs due with Minister's Offices
By day 20	Response sent to requestor

The Ministerial Services team are here to help. You can find out more about us on Kainga: [Ministerial services page \(/people-and-teams/SGE/Pages/Ministerial%20and%20Business%20Services.aspx\)](#)

 **DEPARTMENT OF THE PRIME MINISTER AND CABINET** (http://www.dPMC.govt.nz) FEEDBACK (MAILTO:COMMS@DPMC.GOVT.NZ;WEB.PUBLISHING@CASS.GOV.T.NZ?SUBJECT=DPMC%20INTRANET%20FEEDBACK)
TE TARI O TE PIRIMIA ME TE KOMITI MATUA



(/help-me-with/communications-digital-hub/Pages/Social-Media.aspx)

OIA-requests (/help-me-with/Pages/OIA-requests.aspx) Official Information Act (OIA) Requests

Working with Ministerial Services at DPMC **Document 3**

The Ministerial Services team are part of the Strategy, Governance and Engagement group (SGE) at DPMC. The team is made up of 3 Senior Advisors, 2 Advisors, a Coordinator and a Manger.

THE TEAM IS CENTRALISED... This means almost all OIAs at DPMC are processed by a team of Ministerial Advisors, who are experts in working with the Official Information Act (OIA) 1982 (amongst other things!)

What do we do?

- ❖ Respond to OIA requests received by DPMC, the Prime Minister, and other DPMC portfolio Ministers
- ❖ Process and assist with Ministerial correspondence
- ❖ Coordinate and assist with drafting Written Parliamentary Questions (WPQs)
- ❖ Manage the proactive release of Cabinet material and the publication of OIA responses.

Working together

- ❖ Sometimes the amount of OIA requests, correspondence, and WPQs add additional strain to the capacity of the business group. This often happens when the business group is already busy however, it is important that the **Subject Matter Expert (SME) and business group managers are involved in the decision-making and approval of the release of their own information.**
- ❖ To support DPMC business groups to meet their obligations, **Ministerial Services provides administrative support, manage processes and timelines, and any other reasonable requests for support that is required to progress ministerial work.**

How it works

Ministerial Services will do the heavy lifting in terms of providing administrative support, **working with the SME in the business group** by providing guidance, and advice on the OIA.

The **Ministerial Advisor** will suggest courses of action, undertake administrative tasks, join the dots with other requests, assess risk and help 'shepherd' the request through the sign out process, alongside the SME.

The **SME provides the subject matter expertise** when it comes to content with the **ultimate decision-making/approval of the response** residing with the business unit.

What is Moto?



MOTO is DPMC's **workflow management tool**, which we use to:

- **Track** the progress of OIA requests, ministerial correspondence, Ombudsman investigations, proactive release and other DPMC correspondence as required.
- **Create a record** of each piece of work including who signed out documents, when they were sent to Minister's offices, and when they are returned to DPMC by the Minister's office

Best practice timelines

Day 1	Request received in the information@dpmc.govt.nz mailbox
By day 2	Acknowledged by coordinator and allocated to business group and Ministerial advisor (via Moto)
By day 3	Ministerial advisor assesses requests, ensures the right people are aware, and sets course for response
By day 5	Ministerial advisor confirms proposed timeline and actions to be taken, with business group
By day 7	If required, re-scoping email is sent to requestor
By day 10	<ul style="list-style-type: none">• Documents reviewed and/or processed• Decision made on transfer of requests and preliminary decisions made on need to consult/extend request (if request is to be extended, new timeline and due dates are sent to the relevant people)
Between day 10-15	QA and sign out process commences
By day 15	Ministerial OIA requests are due with Minister's offices
By day 20	Response sent to requestor

For more information on what the Ministerial Services team does, check out our page on Kainga or email us at information@dpmc.govt.nz

Ministerial Services Triage Considerations

Purpose of daily triage is to:

- **Assess risks, sensitivity, and complexity:** Carry out an initial assessment of the risks associated with a piece of work
- **Add value to the business:** Ensure the person accountable for a piece of work is given insights, advice and connections that will assist them
- **Allocate:** Ensure work is allocated correctly
- **Identify SME's to provide QA:** Experts who need to approve the final draft response (e.g., Legal, Finance, media and communications, & Ministerial Services)
- **Join the dots:** Help the whole team to share knowledge, insights and connect issues and pieces of work
- **Advise Executive Director SGE** of the most sensitive items e.g.: all material involving the PM; staff complaints; high profile requests or requesters

A guide to thinking about the complexity, sensitivity, and risks when Ministerial Services staff assess OIA requests, Ministerial letters, and advice is:

Risks or Organisational Impact	Sensitive	Complex	High public interest
<ul style="list-style-type: none"> • Reputational harm to DPMC, Ministers, stakeholders or public sector (e.g., Ministerial conflicts of interest) • Potential harm to staff or an individual (e.g., risk of doxing) • Non-compliance with legislation including: <ul style="list-style-type: none"> ○ OIA, Privacy legislation ○ Cabinet & Parliament rules e.g., due to large or complex requests • Current or impending court proceedings or open investigations 	<ul style="list-style-type: none"> • Highly sensitive or personal material (consider Privacy/personal information) • Complaint about staff or organisation • Protected disclosure 	<ul style="list-style-type: none"> • Inter-connected requests, e.g., WPQs, OIAs, correspondence, briefings • Multiple items/questions included in a single request and high degree of judgement required 	<ul style="list-style-type: none"> • Is this a topic of high public interest, e.g., a controversial decision? • Will there be any significant organisational impact with the information that will be released?
<p>Requestor: Flag if:</p> <ul style="list-style-type: none"> • Media (likely high media interest), • MPs, • Interest groups and repeat requestors 			
<p>NB: Who makes a request may not be necessarily make it high risk; it may simply require Ministerial Services to flag this to the responsible ELT member</p>			

Triage process and outcomes

Ministerial Coordinator will provide an email to the Lead Advisor and Manager Ministerial Services each day (last thing) and include all received OIAs and other correspondence (attach the incoming email with the request)¹.

Lead and Manager will review against the triage criteria and identify prior requests of a similar nature.

Each new item will be discussed in the next daily triage meeting (e.g., items received Monday will be discussed on Tuesday)

OUTPUT - Initial note for the MOTO stickies covering:

- **Assessment of risks, sensitivity and complexity**
- **insights, advice and connections** that will assist them
- **SME's to provide QA**: Experts who need to approve the final draft response (e.g., Office of the CE, Legal, Finance, media and communications, & Ministerial Services)
- **Join the dots**: Help the whole team to share knowledge, insights and connect issues and pieces of work

Triage note template

Ministerial Services Triage Note:

- Requester details
- MS has noted the following risks/sensitivities (*optional and should include a note of need for urgency if appropriate*).
- MS notes the following related workflows and prior response:
 - _____
- MS notes (*any value add – e.g., the PM has publicly responded to this before – link*)
- MS recommend (*comment on approach*)

¹ This will mean a change for the team as the coordinator will not be available to dispatch (externally) responses which are approved/finalised after 4.30pm.

Complaints

Complaints take many forms and need to be carefully considered.

A complaint may be about a service or the actions of a staff member that has resulted in some form of harm or detrimental impact to the complainant.

A complaint needs to be treated seriously and considerations should be made whether it needs to be handled independently.

- Complaints should be discussed with the Manager Ministerial Services

If the complaint includes an OIA then the two elements may need to be treated separately.

Complaints about members of Parliament should be referred to the Cabinet Office (via Manager, Ministerial Services).

Protected disclosure

A protected disclosure is from an employee reporting concerns about a serious wrongdoing in the Department. NOTE: if a protected disclosure is made to the Minister, it may be about an entity other than DPMC.

Serious wrongdoing includes:

- an offence
- a serious risk to public health, public safety, the health or safety of any individual, or the environment
- a serious risk to the maintenance of the law, including the prevention, investigation and detection of offences and the right to a fair trial
- an unlawful, corrupt or irregular use of public funds or public resources
- conduct that is oppressive, unlawfully discriminatory, or grossly negligent, or that is gross mismanagement, by a public sector employee or a person performing a function or duty or exercising a power on behalf of a public sector organisation.

If we see a protected disclosure in the inbox or identify it during triage:

- escalate to Manager Ministerial Services to inform the Deputy Chief Executive Strategy, Governance and Engagement.

Quality Assurance Checklist

Purpose

To produce checklists for the various QA aspects involved in each workflow.

This checklist will serve as a tool/quick reference guide for DPMC when providing QA on others work, and when considering new workflows.

Ensuring consistency in approach to QA and provide assurance that all matters have been checked (i.e., key dates, administrative steps and all questions answered).

Definitions

1. Proofread
 - a. Check greetings
 - b. Confirm dates, email/physical address, and title are correct
 - c. Check structure, grammar, and tone of the response
 - d. Check general formatting of document
 - e. Check that response is tailored to the audience
2. Quality Assure (QA)
 - a. *QA includes a proofread
 - b. Check that concerns/questions raised have been addressed in response
 - c. Confirm internal consultations are completed, and consistent with triage notes
 - d. Check that coversheet appropriately addresses matters raised, and provide a high level summary of any risks involved.
 - e. Check that draft contains a paragraph advising of the right to complain to the Office of the Ombudsman

Preliminary Checks

Advisers should do the following preliminary checks when a piece of work has been assigned to them, prior to commissioning

Things to Check	Notes
Read the request	<ul style="list-style-type: none"> - If you believe it should be logged as another type of work (i.e. if an OIA request has been logged as correspondence), please flag it with the Lead Adviser or Manager immediately
Are the logging dates correct?	<ul style="list-style-type: none"> - For due dates, please use the official information calculator (www.ombudsman.parliament.nz/agency-assistance/official-information-calculators) - Transfer deadlines: no later than 10 working days after the day on which the request is received per section 14 of the OIA
Are internal deadlines, correct?	<ul style="list-style-type: none"> - MOIAs Transfers are due to the Minister's Office 2 working days before the actual deadline - MOIA Responses are due to ELT 2 working days before it is due to the Minister's Office; and are due to the Minister's Office 1 week before the response is due
Is the request document correct?	<ul style="list-style-type: none"> - Make sure that the request document corresponds to the title of the request
Is the sign out team and manager, correct?	<ul style="list-style-type: none"> - While sign outs can change midway through an OIA, it is important to ensure it has been logged against the right business unit/ELT member
Details of requestor*	<ul style="list-style-type: none"> - Check that it corresponds to the request
<p>*For Ombudsman Investigations, please also check that the following details are correctly logged:</p> <ul style="list-style-type: none"> • Details of Ombudsman Investigator • OIA number • Indicative Manager's Sign Out 	
Any previous similar requests?	<ul style="list-style-type: none"> - Run a search on MOTO to see if there have been a previous similar request, and what the approach was - Save the links of the previous requests in the stickies for reference
Should Communications be looped in?	<ul style="list-style-type: none"> - Talk to Manager, Ministerial Services if unsure
Does Legal have to be involved?	<ul style="list-style-type: none"> - E.g. if the request asks for documents containing privileged materials - Where requests seek personal information
Does this need a PAG search?	<ul style="list-style-type: none"> - A PAG search may be required if the request asks for briefings provided to the Prime Minister on a certain matter - Check with Advisers cleared to conduct PAG searches if unsure: <ul style="list-style-type: none"> ○ Anna Whiskin ○ Viv Tan

Not relevant to your request

Transfers & Extensions

This QA checklist applies to both Departmental and Ministerial OIA Requests. The adviser should assess whether communications need to be involved at commissioning.

Relevant Person	Purpose
Adviser or Senior Adviser, Ministerial Services	<ul style="list-style-type: none">- Proofread- QA- If it is a partial transfer, check that the remaining part(s) of the request is addressed- Check if the correct section of the OIA is used- Check length of extension, and confirm it against estimated timeline- Check wording for an extension of transfer deadlines (if necessary)

Official Information Act 1982 (OIA) Requests

This QA checklist applies to both Departmental and Ministerial OIA Requests. The adviser should assess whether legal and/or communications need to be involved at commissioning.

Relevant Person	Purpose
Senior Adviser, Ministerial Services	<ul style="list-style-type: none"> - Proofread - QA - Check if information has been withheld under the appropriate section of the OIA - If it is a full/partial refusal, check if it is made under the appropriate section of the OIA
Policy Advisory Group	<ul style="list-style-type: none"> - Where request involve PAG materials - Confirm the completeness of the scope - Confirm documents in/out of scope is correct
Manager, Ministerial Services	<ul style="list-style-type: none"> - Where necessary
SME, Relevant Business Unit	<ul style="list-style-type: none"> - Proofread - QA - Fact-check use of information, and information proposed to release/withhold
SME's Manager, Relevant Business Unit	<ul style="list-style-type: none"> - Approval on behalf of Business Unit
Legal (where applicable)	<ul style="list-style-type: none"> - Where request involve privileged or procurement information - Where requests are high-risk - Where requests seek personal information
Chief-Of-Staff/Chief Adviser* CPR: Hannah Kerr COVID-19: Julie Knauf Implementation Unit: Maari Porter National Security Group: Christopher Gray NEMA: Anthony Richards	<ul style="list-style-type: none"> - Final checks before it goes to the relevant ELT member for sign out <p>*If the request is for DPMC corporate-related information, this step is not necessary</p>
Communications for oversight (where necessary) CPR: Gabrielle Tully and Sarah Berry PMO: Catherine D. Iore National Security Group: Cherie Blithe	<ul style="list-style-type: none"> - Where matters raised have been in the media or may result in media attention

[Remainder of this Document does not relate to Official Information Act requests and is not relevant to your request]



DEPARTMENT OF THE
PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA



Release of staff personal information under the Official Information Act.

This guide covers how to treat staff names, phone numbers (DDI's and mobiles) and email addresses. As a general rule, both the Ombudsman and the Privacy Commissioner expect names of public service staff, their direct dials and their emails to be released unless there is clear evidence of possible harm to the individual. Redacting work mobile numbers is usually justifiable to ensure people are not contacted outside of working hours.

It is a common misconception that names of 'junior' or 'administrative' staff do not need to be disclosed because there is no public interest in disclosure of that information. However, a harm needs to be established before the public interest in release is considered. If there is no harm, the information must be released, regardless of whether there is a public interest in doing so.

Privacy

Section 9(2)(a) of the OIA applies if withholding is 'necessary to protect the privacy of natural persons'. The Ombudsman has explained their general position that withholding staff names, when all that would be revealed is what they did in their official capacity, is not generally necessary.

"The names of officials should, in principle, be made available when requested. All such information normally discloses is the fact of an individual's employment and what they are doing in that role. Anonymity may be justified if a real likelihood of harm can be identified but it is normally reserved for special circumstances such as where safety concerns arise."

In particular, it will not usually be necessary to withhold staff names or emails in order to protect their privacy. A name is personal information about an individual, but, on its own, that information is not inherently private. Nor is the fact that a person works for an agency, or what they happen to do in that role, inherently private.

A public sector employee should reasonably expect a degree of transparency around what they have done in their official capacity. There is usually no need to withhold employee DDI's, work mobile numbers and work email addresses where it is generally available (for example, because it forms part of staff email signatures which are routinely sent outside the agency), or able to be inferred. For example, agency email addresses often follow a standard formula from which staff email addresses may be readily inferred, if their names are known.

Where the information is not generally available or able to be inferred, there may be a sufficient privacy interest to engage section 9(2)(a), particularly for DDIs and extensions, and work mobile numbers. Work mobile numbers in particular may enable staff to be contacted outside business hours, which would intrude on their personal time. Email contact may be less intrusive than telephone contact, because people can choose if or when to respond to an email.

The sensitivity of any of this information will depend entirely on the context—whether it would, in combination with other information, reveal something private or personal about the individual, or in some other way intrude on their privacy.

Signatures

Assuming a signature is legible, its disclosure might reveal an identity. Even if it isn't, it could be linked to other documents the person has signed. However, that alone is not anything inherently



private, and so it is not ordinarily necessary to withhold signatures and releasing signatures does not necessarily facilitate identity fraud. Usually a signature alone isn't sufficient – the would-be fraudster needs other information (credit card info, date of birth, drivers license number, etc) to do malicious things with a signature.

Improper pressure or harassment

Section 9(2)(g)(ii) applies if withholding is 'necessary to ... maintain the effective conduct of public affairs through ... the protection of [Ministers, members, officers or employees of agencies] from improper pressure or harassment'.

For this section to apply, there should be a reasonable expectation that:

- disclosing the name(s), email, or phone number would lead to improper pressure or harassment; and
- this would have an adverse impact on the relevant staff (for example, by causing stress or anxiety), and therefore the agency's ability to do its job

While there is no onus of proof on an agency to produce evidence in support of a predicted harm, "[any person] *who alleges that good reason exists for withholding information would be expected to bring forward material to support that proposition*". A requester being a persistent or recurrent complainant is unlikely to meet the threshold in the absence of other indications of potential harm.

General factors to consider when assessing whether to withhold this information:

Factors that may affect the need to withhold staff names include the nature and content of the associated information include:

- whether the information is already known to the requester;
- whether the information is in the public domain;
- the seniority of the staff;
- their degree of responsibility;
- the nature of their role;
- their views;
- the potential for further dissemination;
- previous conduct by the requester or others to whom there is a reasonable chance the information will be disclosed; and
- the likely use of the information.

Consulting with other agencies on release of their staff personal information:

DPMC/NEMA needs to consult with the relevant agency regarding its employees and whether names and contact details should be withheld. We recommend you do this by saying:

DPMC/NEMA intends to release the names of all [agency staff], including email addresses and phone details in the attached documents. If [agency] considers there is a real likelihood of harm if the name and contact details were released, please advise by [x date]. If no response is received we will assume [agency] has no objection to the release.



Rationale:

If a business unit makes a decision to redact the names and/or contact details of their staff then the following information will need to be sent to Ministerial Services for their records:

- which specific section of the OIA applies; and
- reasoning or rationale for what the harm would be to the individual staff member if their name and/or contact details were to be released.

A record is important as it enables Ministerial Services to raise the relevant risks with the decision-maker who signs out the OIA and will ultimately own the risk and will need to justify the redactions if a particular OIA goes to the Ombudsman.

The reasoning can be a short sentence or summary of the risk and potential harm. Examples include (but are not limited to):

- The project being worked on is high risk;
- The link between the individual and a particular project or piece of work could disclose their security clearance;
- The requester is known to have a history of harassing employees.

For further information:

The Ombudsman has released a specific guidance document on names and contact details of staff which you can access [here](#) if you would like more information.

If there are questions about how or when the thresholds may be met in specific cases, please get in touch with Ministerial Services.

Released under the Official Information Act