MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

1 July 2022

Tēnā koe

On 20 May 2022, you emailed the Ministry of Social Development (the Ministry) requesting, under the Official Information Act 1982 (the Act), the following information:

- *Any and all documents, that relate to msd privacy policies that staff are given when they are onboarded to their positions, and any other documents that detail, what training they are given, in regard to privacy policies that MSD has in place, and the expectations that are required of staff in relation to those policies, and the consequences if those policies and expectations are not adhered to.*

On 22 May 2022, in addition to the information requested above, you requested the following information under the Act:

- *any and all MSD documents, that detail, what if any, auditing policies and practises MSD has in place in relation to ensuring that people who have access to information held in MSD's systems are complying with the policies as described below.*

On starting employment at the Ministry, all staff are given information and training that relates to privacy. Please find the following enclosed:

- *Code of Conduct,* dated August 2021
- *Online Training Module,* Information Management, Privacy and Security, latest version, as at 20 June 2022.

All staff, permanent and contracted, must acknowledge they have read and understood the Code of Conduct upon being employed at the Ministry. Regular refresher training is also undertaken as part of ongoing staff learning.

The online training module is a scenario-based learning module which covers what information management is and why it is important, protecting information, information privacy and sharing and how to recognise and report

a privacy, information or IT Security breach. It is required learning for all staff.

The Privacy Act 2020 is mentioned in the context of differentiating it to the Official Information Act in the *Official Information Act 1982 training module* document. Please find the relevant segments attached in the **Appendix**.

You may also be interested to see the Ministry's *Acceptable Use of Technology Policy* and *Secure Workplace Policy*, both which are attached in the **Appendix**. The *Acceptable Use of Technology Policy* outlines to staff how to use technology responsibly to keep information and people safe, while the *Secure Workplace Policy* defines information security requirements for the protection of Ministry information held within workplaces and covers staff working from home. Please note these policies are currently under review as per the review dates in the policies.

There is also a Public Privacy Statement available on the Ministry's website at the following link:
www.msd.govt.nz/about-msd-and-our-work/tools/copyright-statement.html#PrivacyStatement3

All Ministry staff have continued access to materials regarding privacy policies to be adhered to by staff.

In regard to your request for information regarding auditing practices, the Ministry has a clear process for Certifying and Accrediting systems or business processes. This includes capturing controls or remediations that may be required to securely manage personal information and ensuring these are followed up and implemented as appropriate. This process includes oversight boards and organisational committees to approve, endorse or recommend actions.

At a high level the Ministry also monitors risks and reports regularly in line with our risk management framework.

Potential consequences if policies and expectations are not adhered to include:

- If staff are in breach of the code of conduct this is usually considered a Human Resources issue, and appropriate investigations and actions would be undertaken by them in this regard.
- If a privacy breach has occurred by a Ministry employee, then the Ministry has established business processes to respond to this. Our staff training and intranet site provide clear instructions for our people on the process to deal with potential privacy breaches. Regular reporting and root cause analysis occurs on breaches to identify any trends and areas where improvement to process or additional training

and consultation may be required. Where required privacy breaches are reported to the OPC if they meet with threshold criteria.

The principles and purposes of the Official Information Act 1982 under which you made your request are:

- to create greater openness and transparency about the plans, work and activities of the Government,
- to increase the ability of the public to participate in the making and administration of our laws and policies and
- to lead to greater accountability in the conduct of public affairs.

This Ministry fully supports those principles and purposes. The Ministry therefore intends to make the information contained in this letter and any attached documents available to the wider public. The Ministry will do this by publishing this letter and attachments on the Ministry's website. Your personal details will be deleted, and the Ministry will not publish any information that would identify you as the person who requested the information.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with this response, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Ngā mihi nui

Hannah Morgan
General Manager
Information

Appendix

Online Training Module – *Ministry of Social Development Official Information Act 1982*

2. A person asking for information about themselves.

The OIA is like a rule book for answering requests for official information. It explains that information must be released unless there is good reason not to. The starting point of the OIA is always openness and transparency.

A person can ask for information about themselves but this isn't covered by the OIA. It is instead covered by the Privacy Act 1993.

An agency has 20 working days to respond to an OIA request

Lesson 4 of 5

The difference between the OIA and the Privacy Act

TS Theresa Stowers

What's the difference between a Privacy Act Request and an OIA Request?

Privacy Act

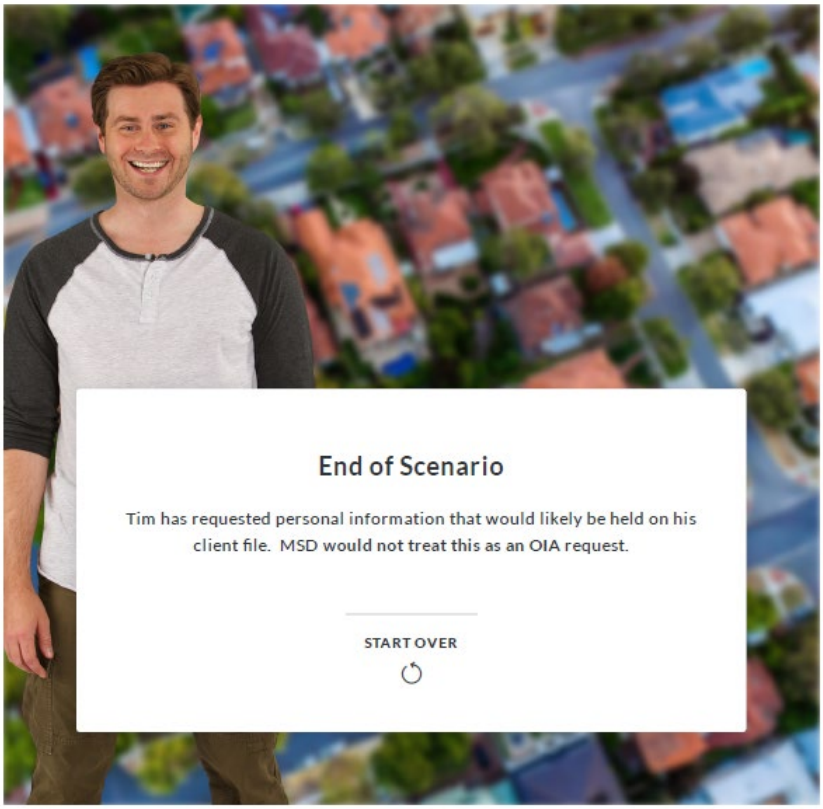
The Privacy Act gives individuals the right to ask any agency (with a few exceptions) for access to the personal information that an agency holds about them. So, if the request is for personal information about the requester, the Privacy Act will apply (even if the information is also official information).

The presumption under the Privacy Act is that individuals will be entitled to their information, unless one of the limited withholding grounds set out in the Privacy Act applies.

Official Information Act

Under the Official Information Act (or Local Government Official Information and Meetings Act), any person or agency may ask a public sector body (or local government body) for any information that agency holds.


I would like to make a request for all of the information that MSD holds on me from when I was receiving Emergency Housing Special Needs Grants. *What act would you apply in this case?*
1 The Privacy Act 1993
2 The Official Information Act (OIA)


End of Scenario
Tim has requested personal information that would likely be held on his client file. MSD would not treat this as an OIA request.
START OVER

Acceptable Use of Technology Policy

All use of technology to store or transfer Ministry information or conduct Ministry business must comply with our Code of Conduct and all relevant laws, regulations, policies and standards. Staff must take particular care when handling client or classified information to keep it safe from unauthorised access, loss or misuse and includes any technology on which it is held or transferred. (See the guideline on Handling official (classified) information).

To safeguard Ministry information and business, staff must:

- Only use technology and applications, including personal devices, with Ministry information where the use is approved. This includes using approved media devices (memory sticks, USBs etc.) to transfer Ministry information and approved tools when working outside of Ministry offices. (See the guidelines on Staying in control of Ministry information which covers keeping Ministry information safe when you need to work away from the office or transfer Ministry information and the IT Guide which covers how to get access to Ministry Tools and Applications or when you need to use other technology or applications.)
- Protect technology and information from loss and misuse by following Ministry standards and guidelines for use and protection of:
    - Ministry passwords and smartcards as they protect access to our information. (See the guidelines on Keeping Passwords Secure and the Managing your Passwords page whenever you need to change a password.)
    - Ministry computers including laptops, tablets and mobiles.
- Report loss of technology when you become aware of it to MSD Service Desk and your Manager and then log the incident in the Incident Reporting System SOSHI.
- Only share Ministry or client information where it is explicitly authorised.
- Only install approved software or technology on Ministry systems where authorised and following related processes. Apps may be downloaded on to Ministry mobile devices from official or approved app stores. (See the MSD Service Desk for the processes covering software, applications and mobility – the mobility link contains the iDevice Guidelines for us of Ministry iDevices).

- Keep safe from malicious attacks (such as suspicious phishing emails, texts or website links) and quickly seek advice from MSD Service Desk for any suspected information loss (for example, if you have been tricked into sharing your password or sent Ministry information to an incorrect recipient). (See the guidelines on Phishing and spam emails and also the public guidance on staying safe online at home by connect smart and netsafe.)

To meet the Ministry's standards of integrity and behaviour (covered in the Code of Conduct) users must:

- Keep personal use of Ministry technology (including emails or internet use) within reasonable limits, making sure it does not interfere with your work or Ministry business (for example over use of email for personal communications or excessive use of resources impacts network or service speeds for other users).
- Never use Ministry information or technology for anything illegal, including infringement of copyright, or objectionable to co-workers, our partners (NGOs) or our clients. (See the information on Copyright Act covering What sort of activities should be avoided, and guidelines covering Inappropriate email use and Inappropriate internet use).
- Use safe practices with personal and work use of social media and avoid damaging the reputation of the Ministry. (See the guidelines on How to keep safe on social media.)

The Ministry proactively monitors the use of technology to keep our information and people safe and manage any impact to our reputation or functions (see the guidelines on Monitoring email and internet use). Where necessary this will include:

- Monitoring private and personal use
- The removal of information where it is offensive or illegal or impacts Ministry business
- The removal of computers as part of disciplinary or criminal investigations.

Secure Workplace Policy

Target Audience

This policy applies to all Ministry staff and contracted service providers.

Policy

Sensitive and personal information should be secured from those who do not have a business purpose for access. This includes other Ministry employees, office visitors and contractors.

MSD's corporate information policy advocates "Digital First" – business information should be digital by default[3].

Any physical information that needs to leave the secure workplace should be transported via secure courier or in a briefcase or similar.

Desks should be cleared of all papers including post-it notes, paper with sensitive information such as account numbers, and non-essential documents.

The secure workplace policy also applies to sensitive and personal information on computers, laptops, DVD or USB drives and mobile devices. Any portable devices should be locked when not in use. This applies to staff who work from home as an extension of their workplace.

Ministry staff at extended periods from their desk, such as a lunch break, should ensure sensitive working papers are placed in locked drawers. Similarly computers, mobile phones and mobile devices should always be in locked mode when you are not using them.

At end of the working day Ministry staff must tidy their desk and put away all office papers and other mobile devices. These papers and devices must be secured in a locked cabinet or drawer.

When documents are no longer needed secure destruction bins must be used to dispose of information.

Staff should be familiar with their obligations when managing Ministry information, whether it is physical or electronic. Information should be managed and stored in an appropriate system such as EDRMS or TRIM. For more on information obligations or using the systems see the Doogle e-learning content and the Information Obligations Quick Guide.

---

[3] This includes creation, distribution, and review. Doing so enables greater accessibility, maintains longevity, mitigates the risk of information loss and reduces duplication.