MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

24 January 2025

Tēnā koe

Official Information Act Request

Thank you for your email of 17 December 2024, requesting information about Ministry policies and procedures around mitigating and reporting privacy breaches.

I have considered your request under the Official Information Act 1982 (the Act). Please find my decision set out below.

I have included the following internal intranet pages which lay out Ministry policy and procedure on requests for personal information, information security and privacy and advice to Ministry staff on information security:

- Privacy and security of information.
- Practical tips to keep information secure.
- How to handle request for personal information.

I will be publishing this decision letter, with your personal details deleted, on the Ministry's website in due course.

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 my decision on your request, 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

pp.

Anna Graham
General Manager
Ministerial and Executive Services

How to handle requests for personal information

This page explains what 'personal information' is, people's rights to access their personal information, and the process for handling access requests. You can find templates to help you manage requests under 'Related links'.

On this Page:

What is 'personal information' about someone?

Personal information is information which tells us something about a specific individual. The information doesn't need to name the person if they're identifiable in other ways.

At te Manatū Whakahiato Ora (MSD) we hold many different kinds of personal information, such as: people's names, addresses and other contact details, birthdates, etc. We may also hold clients' medical, financial, and employment information, and information about their families and living situation.

This information is held in documents, emails, notes, and reports, and is stored in many places including CMS, EDRMS (Objective), physical files, and core systems like SWIFTT, TRIM, and HIYA.

A person doesn't need to be named for the information to be 'personal information'. If the information tells us something about them, and our systems can link it back to them, then it is personal information.

Official information is all information held by MSD.

People have a right to ask for their own personal information

Under the Privacy Act 2020, people are entitled to ask us:

whether MSD has personal information about them, and
for access to any personal information that we hold about them.

We call these 'access requests'.

Where MSD staff are requesting access to their personal information (or official information in a personal capacity), please see this page [http://doogle/business-groups/people-culture-strategy/maes/staff-information-requests.html] for information on how to handle these requests.

Timing

Under the Privacy Act we have 20 working days to respond to access requests. The Office of the Privacy Commissioner's website has a Response Calendar [https://www.privacy.org.nz/your-rights/your-privacy-rights/] to help you work out the response due date on Privacy Act Requests.

There's a limited range of reasons for refusing an access request. For example, some of the information may not be provided if the information would endanger the life or health of the requester or another person. If we refuse an access request, we must still respond to them within 20 working days and let them know we are refusing their request. If you don't know whether the information can be released, or if you think there is a risk that the information might negatively affect the health or safety of the requestor or another person if we release it, whakapā mai at PrivacyOfficer@msd.govt.nz [mailto:PrivacyOfficer@msd.govt.nz] for a kōrero (chat) and some advice.

It doesn't matter why they want it

People don’t have to give us a reason for asking for access to their information. If it’s about them, they’re entitled to get it, unless the law allows us to say no.

They don’t have to spell out what they want

People often ask for “all the information you have about me”.

The Privacy Act doesn’t require them to be more specific and people often can’t be more specific because they don’t know what we hold – that’s why they’re asking.

Talk to the requester

It’s fine to have a kōrero with the person about what they need – that might be helpful for them. They may ask for all the information we hold about them, but in actual fact, they only want to know how we’ve calculated their benefit, or what records we have about their medical history.

By having a kōrero with them you might be able to narrow down the search parameters, which will make it quicker and easier for you to respond to them. But, if they want everything, we must consider their request.

They don’t have to mention the Privacy Act

Requesters don’t always mention the Privacy Act when they ask for their information. Sometimes they get it wrong and talk about the Official Information Act instead.

It doesn’t matter. It’s up to us to know that if they ask for information about themselves, then the Privacy Act applies.

Helpful links when responding to Privacy Act Requests

Requesting Call Recordings

To request call recordings (except when it’s for NZ Police evidential purposes or security incidents), fill in the Business Request for Call Recordings form [http://doogle/helping-you/msd-service-desk/forms-and-requests/business-request-for-call-recordings.html] on Doogle.

An analyst then burns the specified recordings onto a CD and couriers it to the appropriate office/staff member to include with their reply.

You won’t necessarily know the specific dates of the calls or the IDs/staff the requestor wants. In this case, just write the date range and any of the client’s known phone number(s).

Requesting Emails

There’s two parts to this process, depending on what we know about how the individual has been interacting with MSD:

When we know every staff member who would have sent or received emails about the client, we can reach out to the Windows Team in IT, who can carry out searches for relevant emails; or

When we don't know every staff member who has sent or received emails about the client, we can reach out to the Internal Integrity Team in Workplace Integrity, who can use the RAFT system to search for relevant emails.

When you need to know what members have accessed a client's record, use the Audit Request Form [https://doogle.ssi.govt.nz/helping-you/msd-service-desk/forms-and-requests/audit-request-form.html] .

Requesting client information stored within M365

Some client information could be stored within Microsoft 365 (Microsoft Teams; One Drive; Exchange Online; SharePoint or other applications). Email the Information Group te Rōpū Whakamōhiohio at the Information Group [mailto:infohelp@msd.govt.nz] for help extracting this information.

Templates for responding to requests for personal information

Some helpful templates for responding to an access request are linked on the right-hand side of this page.

Kia mahi tahi tātou ki te tiaki i te mōhiohio o ngā iwi o Aotearoa!

Let’s work together to steward the information of New Zealanders!

Content owner: Information Group **Last updated:** 05 November 2024

Practical tips to keep information secure

The Ministry holds and uses lots of information and data about lots of different people. Information is taonga, and as its stewards it is everyone's responsibility to protect it and use it responsibly while it is in our care. Preventing unauthorised access, use, disclosure, manipulation, loss, or theft helps keep information assets safe and available to those who need it. There are lots of easy practical steps and actions you can take to help keep information secure:

On this Page:

Working Space Tips

Always lock your devices when not in use, or when stepping away from your desk (including short breaks or popping to the kitchen). Locking your devices ensures personal and business information is protected from unauthorised access. Locking your computer is as easy as pressing Windows Key + L . Consider setting up fingerprint or facial recognition for faster logging in.

When in public or open plan spaces, information from conversations, phone calls, and computers can be overheard or overseen, leading to loss of confidentiality or privacy. To protect against eavesdropping, consider what people might overhear or see on your device in an open plan office, , and book a meeting room if necessary. Remember that discussing client or business information in a public place like a cafe is not appropriate.

Portable devices like phones or laptops can easily be stolen or lost, risking exposure of the sensitive information stored on them. Ensure you always maintain physical control over devices. Store devices in a locked drawer or locker if you will be away for an extended period of time.

Keep your desk clear of any personal or sensitive paper documents. Don't leave printouts or documents on your desk where it's easy for a visitor or a colleague to accidentally glance over and see it. Storing office papers in a locked drawer at the end of the day is the simplest way to protect information.

Device Security

Do not plug in personal USB devices or charge your mobile phone using its USB cable via your work computer. USB devices can secretly contain malware that execute when plugged into a computer, risking the security of MSD networks, systems, and data.

Do not download any software applications onto your work computer.

Software can secretly contain malware that executes, risking the security of MSD networks, systems, and data.

Downloading any software is therefore strictly prohibited.

If you require additional software on your work computer, follow the IT Software Services request process.

Software may require your manager's approval or purchase approval for any associated costs.

Saving, Storing, and Disposing of Documents

When you've finished working with a hard copy of a document that contains business or personal information, dispose of it in one of our secure recycling bins. This will protect the security of the information and the privacy of anyone it might relate to.

Always use the Ministry's business information repositories to save and store your information, documents, files, and records.

Email Safety

If you suspect that an email you've received is a scam (phishing) attempt, ensure you report the suspicious email by clicking on the 'Report to Servicedesk' button.

Content owner: Information Group **Last updated:** 21 October 2024

Privacy and security of information

Protect the privacy and security of information in accordance with the principles of the Privacy Act, and prevent unauthorised access, use, disclosure, manipulation, loss or theft with our IT systems and tools.

MSD's information takes many forms. It can be stored on our computers, transmitted across networks, printed out, written down, and spoken in conversations. It is one of our most valuable assets. We all have a responsibility to protect the privacy and security of the information we're trusted to manage. Protecting the information of New Zealanders from unauthorised access, use, manipulation, and theft is one of our biggest priorities.

Need to let us know about an incident?

Let us know about a Privacy Incident [https://forms.ssi.govt.nz/ldap_login?orig_path=%2Fforms%2Fnew%3Fform_template_public_name%3DPrivacy%2Bor%2BIT%2BSecurity%2BIncident%2BForm]

Privacy of information

Protecting the privacy of personal information underpins the work we do and the services we provide. We have obligations under the Privacy Act 2020 to protect personal information and we must use information in accordance with the principles of the Act. The principles of the Privacy Act cover all aspects of information management, including its collection, use and disclosure; how we store it, provide access to it, and the correction of it; and how we keep it secure as well as accurate and up to date.

Where information security processes and practices protect information from unauthorised access, good privacy processes and practices protect information from inappropriate use.

When we use information that has been provided to us for a specific purpose, we must only use it for that purpose unless a specified exception applies.

The inadvertent, unintentional, or deliberate compromising of personal information exposes our clients and MSD to a number of risk. By taking basic steps to protect information privacy, we are better able to minimise the likelihood and consequences of those risks.

How to handle requests for personal information [http://doogle/helping-you/information-hub/privacy-and-security-of-information/privacy-of-information/requests-for-personal-information.html]

Examples of a privacy breach [http://doogle/helping-you/information-hub/privacy-and-security-of-information/privacy-of-information/examples-of-a-privacy-breach.html]

Principles of the Privacy Act [http://doogle/helping-you/information-hub/privacy-and-security-of-information/privacy-of-information/principles-of-the-privacy-act.html]

Notify us about a Privacy Breach [https://forms.ssi.govt.nz/ldap_login?orig_path=%2Fforms%2Fnew%3Fform_template_public_name%3DPrivacy%2Bor%2BIT%2BSecurity%2BIncident%2BForm]

Our openness and transparency project

We respect our clients' privacy and are committed to being clear about how we use and share their information.

We have developed material to tell our clients what we do and how we keep information about them safe.

Find out about the openness and transparency work [http://doogle/helping-you/information-hub/privacy-and-security-of-information/privacy-of-information/using-personal-information-responsibly.html] .

Information and IT Security

Information Security is about protecting our clients' personal information and our business information from unauthorised users trying to gain access or make changes to that information. Delivering information security at MSD is guided and monitored by the Information Group, to ensure our information remains protected and secure. The Certification and Accreditation

(C&A) process is owned and administered by the Chief Information Security Officer to ensure that our applications and systems meet MSD's security requirements.

MSD uses IT assets to create, store, use and exchange information. IT Security is the process of implementing measures and systems designed to securely protect those assets and safeguard the information against any unauthorised access, misuse, malfunction, modification, destruction, or improper disclosure, to preserve its value, confidentiality, integrity and availability.

- Practical tips to keep information secure [http://doogle/helping-you/information-hub/privacy-and-security-of-information/security-of-information/practical-tips-to-keep-information-secure.html]
- Managing scam (phishing) and spam emaills [http://doogle/helping-you/information-hub/privacy-and-security-of-information/security-of-information/managing-scam-and-spam-emails.html]
- Keeping your desktop and laptop secure [http://doogle/resources/helping-staff/procedures-manuals/business-security/protection-official-info/desktop-laptop-secure.html]
- Keeping hardware containing MSD information secure [http://doogle/resources/helping-staff/procedures-manuals/business-security/protection-official-info/hardware-secure.html]
- Social media toolkit [http://doogle/helping-you/communications-advice/web-digital/social-media/index.html]
- How to keep safe on social media [http://doogle/working-here/keeping-healthy-and-safe/health-and-safety-in-the-workpalce/personal-safety/how-to-keep-safe-on-social-media.html]
- Using cloud services [http://doogle/helping-you/it-guide/cloud-services/index.html]
- Taking MSD devices for approved International Travel [http://doogle/helping-you/information-hub/privacy-and-security-of-information/it-security/international-travel.html]

Notify a privacy or IT security incident

- Notify a privacy or IT security incident [http://doogle/helping-you/information-hub/notify-a-privacy-or-it-security-incident.html]

Content owner: Information Group **Last updated:** 02 October 2024