



28 April 2025

Tēnā koe

Official Information Act request

Thank you for your emails of 11 and 17 February 2025, requesting information about inappropriate access to client information databases by Ministry staff.

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

- *Any policies and procedures in place to monitor, log, and prevent unauthorised access to these restricted databases.*

The Ministry takes our responsibility to protect the privacy of clients very seriously. All Ministry staff are required to complete training on the Code of Conduct and managing client information.

Instances of potential inappropriate access can be identified through the following mechanisms:

- Clients may request a footprint of access to their file through the Privacy Act;
- Clients may make a complaint to the Ministry about our services, including allegations of inappropriate access or broader complaints.
- The Ministry may have concerns about the performance or conduct of a staff member. An investigation into their access to client systems may take place.

The Ministry also runs a data mining programme that picks up immediately identifiable instances of inappropriate access, where staff members access their own records or the records of known family members.

Please refer to the attached policies relating to unauthorised access:

- Internal Fraud and Corruption Policy,
- Inappropriate accessing and processing of information, and
- Dealing with information.

The Ministry's Code of Conduct is available online, here:

www.msd.govt.nz/documents/about-msd-and-our-work/publications-resources/official-information-responses/2022/march/30-3-2022-request-for-copy-of-msd-s-internal-policies-including-code-of-conduct-and-overlapping-duties-of-care-policy-msd-code-of-conduct-.pdf. All employees are bound by the

Code of Conduct. Please refer to page 11 of the Code of Conduct for information specific to inappropriate access.

- *Staff Access Logs:*
 - *I am specifically requesting logs for unauthorised access to client information databases (such as the CMS system), not all restricted databases. If possible, please limit the request to the last 12 months or any significant incidents that occurred within this period.*
- *Unauthorised Access Incidents:*
 - *I would like to request data on unauthorised access to client information within the CMS system in the past three years. Specifically, I am seeking information on the number of incidents, the type of unauthorised access (e.g., attempts to access records), and the actions taken in response.*

Please see the attached **Excel spreadsheet**, which contains the following information:

- **Table One:** The number of investigations into inappropriate accessing in the period 1 January 2022 to 31 December 2024, broken down by quarter ending.
 - This table only covers inappropriate accessing that is identified through the Ministry's data mining programme.
- **Table Two:** The number of completed Employment Relations (ER) cases relating to inappropriate access in the period 1 January 2022 to 31 March 2025, broken down by ER case type and quarter ending.
- **Table Three:** The number of completed Employment Relations (ER) cases relating to inappropriate access in the period 1 January 2022 to 31 March 2025, broken down by outcome and quarter ending.

Please note that some information is withheld under section 9(2)(a) of the Act in order to protect the privacy of natural persons. The need to protect the privacy of these individuals outweighs any public interest in the release of this information.

In the period April 2024 to March 2025, there were 8,044 unique CMS users accessing CMS, including automated system use. Given the total number of times that client files are accessed each year, a very small percentage of overall access to client files is inappropriate. Where an instance of inappropriate access is identified, the Ministry takes the appropriate action in relation to those staff members.

The Ministry is not able to provide you with information about the total number of instances of inappropriate access within the last three years. In order to provide you with this information, the Ministry would need to manually review the access history of every client file within the requested period.

As such, your request for the total number of instances of inappropriate access within the last three years is refused under section 18(f) of the Act, as substantial manual collation would be required to provide this information. The greater public interest is in the effective and efficient administration of the public service.

I have considered whether the Ministry would be able to respond to your request given extra time, or the ability to charge for the information requested. I have

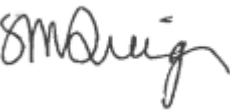
concluded that, in either case, the Ministry's ability to undertake its work would still be prejudiced.

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 regarding inappropriate access of client information, 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

pp. 

Anna Graham
General Manager
Ministerial and Executive Services

Home » Working here » Working for us » Standards of integrity and behaviour » **Dealing with information**

Dealing with information

All Ministry business units hold personal information of some kind, whether it relates to external clients or staff. This page describes the approach staff should take when dealing with information of a personal and sensitive nature.

As Ministry staff and public servants we are all responsible for maintaining and upholding the integrity of the Ministry and its systems. Not only does this protect our reputation and credibility with government, clients and the public, but it also provides us all with a safe and honest workplace.

Information of a personal and sensitive nature should be treated with the utmost confidentiality and not revealed to anyone unless:

you have specific authority from the person providing the information
you have specific authority from your manager
the information relates specifically to the Ministry's work / client base.

We must all take reasonable care to ensure that Ministry and client information is only accessible to authorised people for authorised purposes. It must be kept in a physically safe location. When we do access information it should only be on a "Need to Know" basis.

Some examples of what we should not do are:

look up a relative's or friend's address for another family member or friend
look up birth dates or tax numbers for family, friends or others that are not part of your case load.

Other non-personal information can be extremely sensitive and must not be accessed or released without the appropriate authority.

Mental Health Condition:

It is important that where a mental health condition may be a factor, managers read the Ministry's guidance on managing performance issues which may result from the mental health condition.

Prior to any action being taken, such as talking to, meeting with or writing to an employee, managers must seek advice from the HR Consultancy team.

[Mental Health Guidelines \(PDF 331.84KB\)](#) [http://doogle/documents/resources/helping_staff/forms_templates/hr/mental_health_guidance-gmhr.pdf]

[Read our staff Code of Conduct](#) [<http://doogle/working-here/working-for-us/standards-of-behaviour/codes-of-conduct/msd-code-of-conduct.html>]

[Learn more about our Zero Tolerance policy to staff fraud and misuse of information](#) [http://doogle/resources/helping_staff/policies-standards/hr/zero-tolerance-policy.html]

Content owner: [Human Resources](#) Last updated: 29 November 2020



Inappropriate accessing and processing of information

What does inappropriate access to client information mean?

It means that an MSD staff member has looked at client information held by MSD (usually within the client management and MSD payment systems) without authorisation.

What use is never authorised?

- The information you access and view must be for legitimate work purposes, aligned to the functions of your role.
- You should never access any kaimahi record within the Ministry, including your own.
- You should never access any record of a friend, relative, or acquaintance.

What might inappropriate access look like?

Accessing information about:

- public figures that are in the media
- whānau and extended whānau and/or people that you know. This can also include people you are connected with on social media, sports clubs and/or other online activities
- external business and/or business undertaking with which you are affiliated with.

Sometimes things can unintentionally go wrong, e.g. an email is sent to the wrong address. If you notice a privacy incident like this, let a Manager know as soon as possible.

Why do I need to have a legitimate purpose?

- If MSD provides unauthorised access to a client's information, MSD is breaching that client's privacy under the Privacy Act 2020. If kaimahi have no legitimate business reason to access a client's record, access is unauthorised.
- You are a Public Servant and have access to MSD knowledge and systems that the public and our clients do not have. You must not abuse your position.
- You must treat the information imparted to us by our often vulnerable clients with care and only use it for its proper purposes. You should always be mindful of people's right to privacy in their dealings with the Ministry.
- We need to make sure we are always fair in the way we deal with people. We must avoid any appearance or suggestion of preferential treatment or favouritism towards any individual or organisation which we or you have an interest in.

- This means you also need to avoid doing any work with friends, relatives, or acquaintances as it could give rise to a perception of favouritism and a better level of service. This would also be a Conflict of Interest.

Remember, it's not only about how you see the relationship, but also how a member of the public might perceive it.

What do I do if I have accessed information that I should not have?

1. Exit the record/file immediately.
2. E-mail your manager immediately.
3. Report the incident to the Information Group via PrivacyOfficer@msd.govt.nz.

Accessing my own information

You can get access to your information by:

1. Talking to your manager
2. E-mailing the Privacy Team with your request at PrivacyOfficer@MSD.govt.nz.

What can I do to prevent inappropriate access?

- If you are unsure about accessing a client's information, talk to your manager.
- As a kaimahi you are also able to apply for income support assistance through our Staff Assistance Unit on 0508 673 933. They can talk you through possible entitlements and any ongoing income support that might be available.

Where do I go if I suspect inappropriate access?

- Contact Internal Integrity at internal_integrity@msd.govt.nz or call us on 0508 444 001.
- Contact Employee Relations and your local HR Consultant.
- Get advice from your Regional Integrity Specialist Integrity Services - Doogee.

Other useful reading

Be familiar with our Internal Fraud and Corruption Policy.

Employee Assistance Programme (EAP) provides professional support with a qualified healthcare professional. It is an independent and confidential programme there to assist you if you or your family are experiencing any personal or work-related difficulties.

Internal Fraud and Corruption Policy

Last Review Date:	New policy – May 2019
Next Review Date:	May 2022
Approved by:	Organisational Integrity and Capability Governance Committee
Owner:	General Manager, Workplace Integrity

Purpose

This policy outlines how the Ministry will deal with instances of alleged fraud and corruption. It explains staff's responsibilities to prevent fraud and corruption and the procedures to follow where fraud or corruption is suspected. It confirms that fraud and corruption are considered to be serious breaches of the Code of Conduct and serves to reinforce that fraud and corruption are unacceptable within MSD.

Policy Statement

This fraud policy defines the standards and expectations for Ministry staff (including temporary staff), managers and contractors in relation to fraud and dishonest behaviour. This policy should be read in conjunction with the Code of Conduct.

Scope

This policy applies to all Ministry of Social Development employees and contractors for all Ministry activities and, as applicable, any other activities for which the employee or contractor has a direct management or functional responsibility.

Policy Principles

- Ministry staff will act with honesty and integrity at all times to meet code of conduct requirements.
- Allegations or suspicions of dishonest behaviour or fraud will be treated confidentially and investigated promptly to a natural conclusion.
- When fraud or other dishonesty behaviour is discovered the Ministry will ensure that it is taken seriously and all incidents are formally assessed and investigated.
- When employee dishonesty, misappropriation of assets or fraud is found, this is viewed as serious misconduct and the appropriate disciplinary action will be taken.
- Legal action will be taken against those committing fraud, including referral to the Crown Solicitors or the New Zealand Police.

Assessment of Suspected Fraud

Suspected incidents of fraud and dishonesty will be assessed and then investigated by the Internal Integrity.

The Internal Integrity will:

- Investigate all cases of suspected fraud or corruption in a professional manner
- Interview a number of people, ranging from the complainant, witnesses and the staff member/s in question
- Access Ministry systems to gather evidence needed for the investigation
- Examine all evidence gathered carefully and thoroughly to determine if fraud occurred

- Refer all proven cases of fraud or corruption to the Crown Solicitors or the New Zealand Police.
- Advise the staff member, their manager, and Human Resources of the Investigation outcome in writing.

Governance Reporting:

The Manager – Internal Integrity will report on the unit's activities, including any trends, on a quarterly basis to the relevant Ministry Governance Committee and the Risk and Audit Committee (RAC).

Responsibilities

The focus on preventing and managing internal fraud is an across Ministry responsibility. Individual roles have different parts to play in ensuring that the wider system is appropriately managed.

These roles are described below:

Person/Party	Responsibilities
Leadership team	<ul style="list-style-type: none"> • Overall responsibility for fraud and corruption management within the Ministry
Managers	<ul style="list-style-type: none"> • Demonstrate and require others to demonstrate high standards of integrity as set out in the Ministry's Code of Conduct • Ensure all employees understand what behaviours are expected and what is unacceptable behaviour • Ensure staff are aware of the policies, controls and assurance systems within their particular role • Reinforcing ethical behaviour within their team or group • Deal with fraud and dishonesty allegations in accordance with Ministry policy and procedures. • Implement and adhere to appropriate internal controls. This could include monitoring transactions, activities or other systems that may be susceptible to fraud or corruption.
Staff and Contractors	<ul style="list-style-type: none"> • Demonstrate high standards of integrity as set out in the Ministry's Code of Conduct • Be aware and comply with the Code of Conduct. • Report allegations or suspected incidents of dishonesty immediately • Alert their manager where they believe the opportunity for dishonest behaviour exists because of poor procedures or lack of effective controls • Cooperate fully in any investigation by providing all relevant information and participating in interviews

Definitions

Word/ phrase	Definition
Fraud	<p>Fraud is intentional deception or misappropriation of funds, in both financial and non-financial domains. It generally has the objective of obtaining an advantage or benefit for the perpetrator, or to cause intentional damage or loss to others. Examples of fraud include, but are not limited to:</p> <ul style="list-style-type: none"> • Benefit Fraud • Creation and use of forged documents • Unauthorised alteration of official documents • Falsifying timesheets, expense claims or leave records • Fictitious employment and qualification credentials • Unauthorised payments in the Ministry's financial systems
Corruption	<p>Corruption occurs where an individual abuses or misuses their position of power, authority or trust for illegitimate personal gain. Examples of corruption include, but are not limited to:</p> <ul style="list-style-type: none"> • Accepting a gift or kickbacks in return for the provision of Ministry services or withholding of Ministry services (bribery) • Showing favour to family and friends in relation to employment decisions or Ministry business (conflict of interest) • Using position of power to exert undue influence on matters beyond the jurisdiction of authority (extortion)
Misappropriation	<p>Misappropriation is unauthorised use of assets and resources for personal benefit or gain. Examples include, but are not limited to:</p> <ul style="list-style-type: none"> • Outright theft of cash or property • Misuse of Ministry resources for personal benefit • Selling or disclosing Ministry and client information for personal benefit or gain to unauthorised parties • Using Ministry systems to issue fraudulent payments for personal purchases, fictitious clients or vendors, ghost employees and fraudulent invoices.
Internal controls	<p>Systematic measures (such as reviews, data mining, checks and balances, methods and procedures) instituted to enable the Ministry to:</p> <ul style="list-style-type: none"> • Deter and detect errors, fraud and theft • Ensure accuracy and completeness • Ensure adherence to policies and plans • Safeguard its assets and resources • Produce financial information that is timely and reliable

Dishonesty	<p>Dishonest behaviour, deceit, or acting without authority, including fraud and corruption. Examples of dishonesty include, but are not limited to:</p> <ul style="list-style-type: none"> • Theft • Lying or being deliberately deceptive • Fraud • Misappropriation of information • Lack of probity
Investigation	<p>An investigation is a methodical and specialised process of discovery to:</p> <ul style="list-style-type: none"> • Prove whether fraud, corruption, theft or other dishonest behaviour occurred • Gather forensic evidence to support a prosecution • Quantify impact and losses incurred

Related policies

Word/ phrase	Definition
Code of Conduct	<p>The Ministry's Code of Conduct outlines our responsibilities in terms of conduct, conflicts and compromise, and the State Services Standards of Integrity and Conduct provides overarching principles. This policy supports those responsibilities and principles. It is intended to assist managers and employees to think about the issues and work through the processes appropriately.</p>
State Services Code of Conduct	<p>Seeks to reinforce a spirit of service and sets common standards of behaviour required from the diverse range of people and roles across the State Services.</p>

Appendices

- **Appendix 1:** *Code of Conduct*
- **Appendix 2:** State Services Code of Conduct