



09 MAR 2021

On 2 February 2021, you emailed the Ministry of Social Development (the Ministry) requesting, under the Official Information Act 1982 (the Act), the following information:

- *Copies of the Ministry's policies for staff relating to the use of social media, working from home including health and safety policy, use of work phone and company vehicle, forming of sexual or personal relationships in the workplace, speaking to media, voicing political views and vaccinations.*

On 9 February 2021, the Ministry contacted you to clarify the below parts of the request with you.

- *Forming of sexual or personal relationship in the workplace.*
- *Vaccinations.*

That same day, the Ministry received a response from you advising of the below clarification:

- *Referring to Ministry staff relationship with each other, not Ministry staff with clients.*
- *Any policy that the Ministry has in place regarding the COVID-19 vaccination, or any other vaccination.*

It is important to note that the Ministry does not have a working from home policy but does have remote working and flexible working policies.

- **Remote working:** This is where staff members are not in a Ministry office full time but work primarily from a location other than an MSD site, for a specified term, in response to a business needs. This could include other Government agencies or the employees' home.
- **Flexible working:** Flexible working can include different work hours, leave patterns, location of work, or flexibility within a role. Flexible working arrangements will need to fit with the Ministry's responsibilities, with the team's functions and deliverables and the employee's role. Flexi-place is a flexible working option that allows employees to work from locations other than their designated workplace, such as working from home regularly or from time to time.

The Ministry is providing you with a copy of the named Policies listed below to answer your request. It is important to note that some of the policies cover multiple parts to your request.

- *Code of Conduct*, dated July 2011
- *MSD Social Media Policy: for the use of social media in an official capacity*, dated December 2020
- *Social media use in the workplace*, dated December 2020
- *Using the internet*, dated August 2016
- *Staying safe online*, dated December 2017
- *Ministry of Social Development Information Security Policies*, dated March 2017
- *Flexible Working Policy*, dated January 2021
- *Remote Working Policy*, dated November 2020
- *Health, safety and security when working from home*, dated February 2021
- *Off-site-safety-and-security-policy*, dated September 2016
- *Motor vehicles policy*, dated July 2020
- *Positive Workplace Behaviours Policy – Addressing harassment and Bullying*, dated December 2019
- *Media policy*, dated February 2020
- *Conflict of values, interests and politics policy*, dated July 2019
- *MSD Flu vaccinations*, dated February 2021

You may note that some information has been 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 this information.

Please note that some information has also been withheld under section 9(2)(g)(ii) of the Act for the protection of such Ministers, members of organisations, officers and employees from improper pressure or harassment.

In regard to your request for the policies for use of work phone, forming of relationships and the COVID-19 vaccinations, this information does not exist and is therefore refused under section 18(e) of the Act. The Ministry, however, has provided you with the guidance for each part of the request that was refused, as outlined below.

### **Use of work phones**

In regard to the use of a work phone, Ministry staff must comply with the Code of Conduct and all relevant laws, regulations, policies, and standards. To safeguard Ministry information and business, staff must only use technology and applications with Ministry information where the use has been approved. This includes using approved media devices (eg memory sticks, USB) to transfer Ministry information and approved tools when working outside of Ministry offices.

Only applications that are on the Ministry's approved software list can be downloaded onto a work phone. The Ministry has a mobility link that contains the iDevice Guidelines for all use of Ministry iDevices.

The Ministry proactively monitors the use of technology to keep our information and people safe and manage any impact to the Ministry's reputation or functions.

### **Forming of sexual or personal relationships in the workplace**

The Ministry does not have a set policy in regard to relationships forming in the workplace. However, there are expectations that are set out in the code of conduct that has been provided to you. The Ministry has provided you with two other policy that relate to this part of your request, Positive Workplace Behaviours Policy – Addressing Harassment and Bullying and Conflict of values, interest, and politics policy.

### **Vaccinations**

The Ministry has provided you with the MSD Flu vaccination policy, however, in regard to the COVID-19 vaccinations there is no current policy or procedure that has been confirmed. The Ministry will follow the guidance of the Ministry of Health and the Public Services Commission.

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

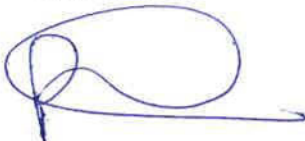
- to create greater openness and transparency about the plans, work, and activities of the Government,
- to increase the ability of the public to participate in the making and administration of our laws and policies and
- to lead to greater accountability in the conduct of public affairs.

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 of Social Development'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](mailto:OIA_Requests@msd.govt.nz).

If you are not satisfied with this response in regard to the policy's that the Ministry have, 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](http://www.ombudsman.parliament.nz) or 0800 802 602.

Ngā mihi nui



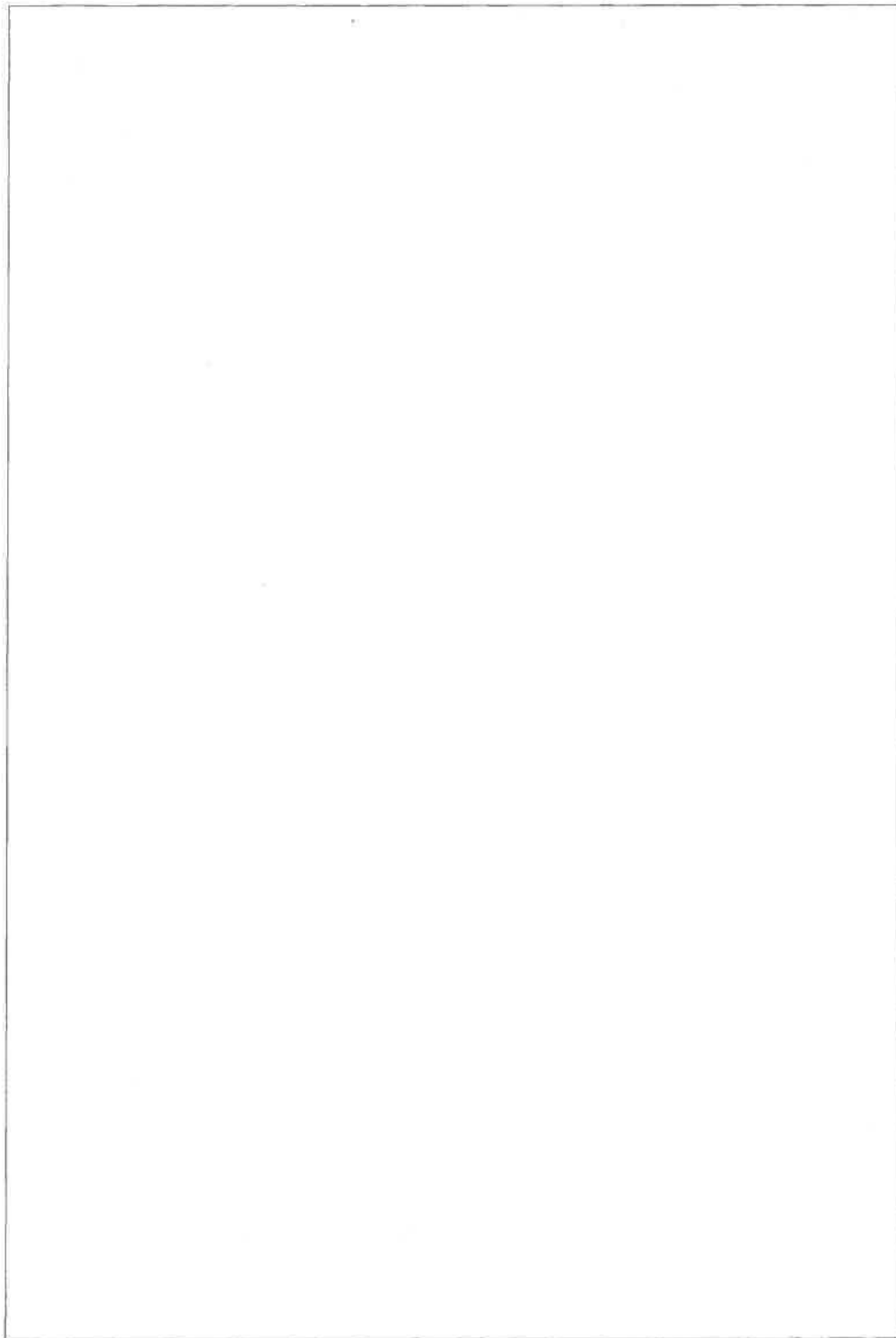
Penny Rounthwaite  
**Group General Manager People**

# ➤ Code of Conduct

July 2011



MINISTRY OF  
SOCIAL DEVELOPMENT  
*Te Manatū Whakahiato Ora*





# Introduction

As public servants we have a privileged role. Each of us has the opportunity to make a positive difference in the lives of New Zealanders through the work we do.

So we can do our work, the taxpayers of New Zealand entrust us with the stewardship of their money, they trust us to protect their personal information and in some cases they trust us to be responsible for the care and protection of their children.

This is a big responsibility. It is important that the way we conduct ourselves reflects the trust New Zealand citizens place in us.

That's why we have a Code of Conduct. This Code provides you with guidelines on how to go about your work and how to best serve the government of the day. It is important you are familiar with the Code and you read it regularly. In fact, it is a requirement if you work here.

The Ministry of Social Development has a responsibility to you to be a good employer. You have the right to be treated fairly in all aspects of your job.

In return, there are some things the Ministry expects from you. The Code of Conduct includes clear expectations about behaviour and conduct we cannot and will not tolerate, and the consequences of not meeting these expectations. The Code clearly outlines the consequences of staff fraud, the deliberate release of sensitive information to third parties without authorisation, and sexual contact with, or abuse in any way of, children or young people the Ministry has a professional relationship with.

The Code of Conduct is a guide for you. It won't cover every situation or requirement you experience in your role. If you are ever unsure about what to do, ask for help.



# Contents

About the Code of Conduct .....	1
Coverage .....	2
Standards .....	2
Zero tolerance .....	3
Fair .....	4
Conflicts of interest .....	4
Respecting others .....	5
Impartial .....	6
Political neutrality .....	6
Commenting on government policy .....	6
Private communications with Ministers or Members of Parliament .....	7
Standing as a Member of Parliament .....	7
Responsible .....	8
Probity .....	8
Information and confidentiality .....	9
Accessing information .....	10
Misuse of information .....	10
Trustworthy .....	11
Client relationships .....	11
Fraud .....	12
Prior or pending convictions .....	12
Gifts and rewards .....	13
Other work or services .....	13
Staff who are also clients .....	13
Breaches of the Code of Conduct .....	14
Reporting breaches of the Code of Conduct .....	14
Reporting serious wrongdoing .....	15
If you think the Ministry has not met its obligations under the Code .....	15
If you breach or think there is a risk you could breach the Code .....	16





# 7 About the Code of Conduct

The Code of Conduct tells you about the way we work. It outlines how we should deal with the people we work alongside and the people we work for, to help make sure we all:

- work with honesty, integrity and respect
- provide the best possible service and advice to the Government, public and clients, and gain their trust and confidence in what we do
- do the best we can do and be the best we can be – every day.

This Code doesn't cover every possible requirement or situation. It gives us a benchmark to work from and gives others a basis from which to judge the way we are working.

We have policies and procedures that give you more detail on the way we work. You should understand and act on the policies and procedures that apply in the Ministry. You can find these on our intranet. If they change we'll let you know – meanwhile, read the Code and understand its contents.

Please note, if you don't meet these standards of conduct your behaviour may result in disciplinary action which could include termination of employment.

It is important you fully understand the Code. If you have questions about parts of the Code and how they apply to you in your role, or you are uncertain as to what some of the information means, ask your manager to explain.

## Coverage

The Code applies to anyone who works for us, including:

- employees
- contractors
- consultants
- volunteers at the Ministry.

Whether you are a permanent staff member, are here temporarily or casually, or are a full-time or part-time worker, the Code applies to you.

The Code is part of your employment terms and conditions. It should be read alongside your employment agreement or contract, our policies and procedures, and the State Services Standards of Integrity and Conduct.

## Standards

The State Services Commissioner has issued the State Services Standards of Integrity and Conduct. This document sets out the minimum standards of behaviour expected of public servants and is issued under section 57 of the State Sector Act 1988.

The standards say we must be:

- fair
- impartial
- responsible
- trustworthy.

You can find them in more detail at [www.ssc.govt.nz/code](http://www.ssc.govt.nz/code).

The following pages outline what these standards mean for us as part of the Ministry of Social Development, and what policies and procedures help us to comply with them.

## 7 Zero tolerance

All public servants are expected to uphold general standards of behaviour. In the Ministry, there are higher standards over and above these in some areas because of the work we do.

The Ministry of Social Development is responsible for paying benefits and for prosecuting those who defraud the benefit system. Every day some of our staff use statutory powers to remove children from adults who abuse them. Our clients are required to provide us with highly sensitive, personal information to get what they need, or for our business reasons. This means that in these particular areas the standards we apply to ourselves must be higher than those we expect of others.

It is unacceptable under any circumstances for a Ministry staff member to:

- steal from the benefit system or the Ministry
- interfere with or in any way abuse a child or young person we are responsible for
- sell client information
- share client details or circumstances with someone outside of work without proper authority.

In every case where a staff member is caught doing any of these things, the staff member will be dismissed and in every case the matter will be referred to police. In addition to any penalty the Court might impose, all money fraudulently obtained will have to be repaid in full.

Specific applications of the Ministry's zero tolerance policy are in the following pages. You can find other information in relevant Ministry policies on our intranet.



# Fair

## Conflicts of interest

At the Ministry we need to make sure we are always fair in the way we deal with people, no matter who they are, what their backgrounds are or what their needs are.

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.

Because we live and work in our communities, it is sometimes hard to avoid conflicts of interest, whether real or perceived. That makes it even more important that conflicts of interest are identified and managed when they can be, and avoided when they cannot.

The Ministry has a policy and a procedure to help you and your manager identify and manage conflicts of interest that arise in the course of your work. You can find the policy and procedure for managing conflicts of interests on the intranet.

You must inform your manager if you have a relationship with someone you deal with in your role or someone we deal with at the Ministry that could cause or be seen to cause a conflict of interest.

Because we live and work in our communities, it is sometimes hard to avoid conflicts of interest, whether real or perceived. That makes it even more important that conflicts of interest are identified and managed when they can be, and avoided when they cannot.

## Respecting others

As a Ministry staff member you need to make sure you respect the rights of other people, all the time. This includes any client, colleague or member of the public.

In particular, you must:

- ensure any workplace relationships with colleagues don't have a negative effect on your work
- respect others' dignity and worth
- not bring anything to work that could be seen as offensive to any person or group of people
- always be professional and unbiased in the work you do, or the advice you give
- be fair and unbiased, no matter who you are dealing with
- not bully, intimidate or threaten others
- remember that everyone has the right to privacy and confidentiality
- avoid acting in a way that could upset people, or cause harm or disruption
- make sure you don't abuse your position at the Ministry, or any power delegated to you in your role.

We understand that sometimes you may need to do something as part of your role that conflicts with your personal beliefs. If you find yourself in this position, talk to your manager. They will be able to discuss this with you and help you find the right solution.

# Impartial

## Political neutrality

While we work with the government of the day, we must also be able to work with future governments. This means we need to maintain the confidence of our current Minister and make sure the same relationship can be established with future Ministers. We do this by keeping politics out of our work and our work out of politics.

As public servants, we have the same rights as other New Zealanders and may publicly express our own political or personal views. However, at the same time we need to maintain our political neutrality. For most of us most of the time, this isn't difficult. For some of us, such as senior managers who work closely with Ministers, we have to keep a balance and it is not appropriate to publicly express views about government policy.

The State Services Commissioner's guidance about political neutrality is available at [www.ssc.govt.nz](http://www.ssc.govt.nz) or you can talk to your manager if you have any questions about what this means for you.

## Commenting on government policy

You should not publicly comment on government policies. The Ministry may view staff members who make strong public statements or repeated criticisms of government policies as being unable to impartially implement, administer or advise on government policies.

Only people who are authorised by the Chief Executive or who have permission as part of their job can make public statements. This applies to responses to any media enquiry.

## **Private communications with Ministers or Members of Parliament**

You have the same right to approach political representatives as any other person, but you must remain politically neutral. Remember, any approach to a political representative about something that is not to do with the Ministry's work should be made with some sensitivity to your role as a public servant.

Any matters concerning the Ministry must go through the official Ministry channels.

## **Standing as a Member of Parliament**

Public servants can seek election to Parliament but there are rules about this set out in the Electoral Act 1993. If you are thinking about putting your name forward for nomination as a constituency candidate or for inclusion on a party list, or if you have already done so, tell your general manager, regional commissioner or the General Manager Human Resources. They will discuss this with the Chief Executive.

You can find more information on the State Services Commission website [www.ssc.govt.nz/code](http://www.ssc.govt.nz/code) and in the State Services Standards of Integrity and Conduct.



# ➤ Responsible

## Probity

When we deal with public money and resources, there is a standard of behaviour expected of us. This is called probity.

Probity means we have shown integrity and professionalism in using public money to do our work.

Probity isn't about setting a list of rules; it's about showing we have used good judgement and a sensible process to make our decisions around how we spend money.

When spending public money, you can show probity if your expenditure:

- is reasonable
- demonstrates value for money
- is relevant to what we do, or to our goals
- can satisfy the questions of anyone who asks about it, including the public.

If you have questions about probity or how to apply it in your role, talk to your manager.

The Ministry's financial policies are available on our intranet.

## Information and confidentiality

We need to keep all Ministry information secure, including personal information about our clients, their families or their organisations.

How we treat this information – collect it, store it, share it and use it – affects how the public trusts us and whether they are willing to continue to share their information with us so we can do our jobs properly.

The Ministry has a number of policies and procedures in place to protect information and to help us manage information appropriately.

This includes complying with the:

- Official Information Act 1982
- Privacy Act 1993
- Public Records Act 2005.

You can find more information about the Ministry's IT policies on our intranet, particularly the Ministry's End User Security Policy.

We need to keep all Ministry information secure, including personal information about our clients, their families or their organisations.

## Accessing information

Each of us must take care to ensure Ministry and client information is only accessible to authorised people for authorised use.

Make sure you always observe people's right to privacy when you are dealing with their personal information.

- You must only access client information or records for legitimate work purposes.
- You must not access your own record or the record of a friend, relative, colleague or acquaintance for any reason, even if the person asks you to.
- Accessing information also includes processing actions on records. You must not undertake any processing action within your own record or the record of any current or former client, including your own record if you're a current or former client of the Ministry, without a legitimate business reason – even if you're just interested or browsing.

This applies to any information we hold in any form. If you are not sure whether it is appropriate for you to access information, always check with your manager first.

## Misuse of information

If you are found to have misused or falsified Ministry information, formal disciplinary action will be taken, which may include dismissal.

The Ministry has a zero tolerance policy for the misuse of personal information. Any staff member found to have sold or given client information to someone without proper authority will be dismissed and the matter will be referred to police.

Any staff member found to have released or distributed information of a sensitive or confidential nature without proper authority will be dismissed.

You can find more information about this on our intranet.

## 7 Trustworthy

### Client relationships

When we work for a government department it is important to be aware of how our relationships can affect the way we do our jobs or the reputation of the Ministry.

You must inform your manager if you have a relationship with someone you deal with in your role or someone we deal with at the Ministry that could cause, or be seen to cause, a conflict of interest.

Disclosing and managing these relationships is important to ensure the public's trust in the Ministry is well-founded and conflicts of interest are appropriately managed.

The Ministry has a vital role in protecting vulnerable children and young people. Because of this, we have zero tolerance for staff who interfere with, or in any way abuse, a child or young person we are responsible for. If you have sexual contact with, or abuse in any way, a child or young person we have a professional relationship with, you will be dismissed and the matter will be referred to police.

You must inform your manager if you have a relationship with someone you deal with in your role or someone we deal with at the Ministry that could cause, or be seen to cause, a conflict of interest.

## Fraud

As a Ministry staff member, you must not commit, condone, encourage or be directly associated with any type of fraud.

The Ministry has a zero tolerance policy for fraud. In every case where a staff member is found to have defrauded the Ministry, they will be dismissed and the matter will be referred to police. In addition to any penalty the Court might impose, all money fraudulently obtained will have to be repaid in full.

If you know, or think you know, that someone is involved in fraud against the Ministry, tell your manager, the Internal Fraud Unit or Integrity Services.

If you are a social worker and you believe or know someone you deal with professionally (including any of their relatives or associates) is getting a payment from the Ministry they are not entitled to, you must tell the person they need to let us know about any change of circumstances that could affect that payment. If you think by doing this you might be placing a child, young person, their family or the work you've been doing with the family at risk, talk to your manager.

## Prior or pending convictions

If you have a conviction we didn't know about before we hired you, or you weren't truthful about, we may take disciplinary action which could result in dismissal.

This does not apply to anything covered by section 7 of the Criminal Records (Clean Slate) Act 2004.

You must tell your manager if you have any convictions or criminal charges laid against you while you work for the Ministry.

## Gifts and rewards

Any form of gift or reward for doing your role could be seen as a bribe or as a way of making you obligated to another person or organisation.

As a general rule you should not ask for or accept a gift or reward. Some occasions (such as a hui) may require an exchange of gifts. We are committed to meeting the needs of different cultures and if a gift is offered in these situations, it should be accepted on behalf of the Ministry. If you are in this situation, discuss it with your manager.

For more detail, refer to the Ministry's financial policies.

## Other work or services

If you take on other work or services while you work at the Ministry, you'll need to consider how it could affect your work here. Make sure it doesn't conflict with your duties, negatively affect your performance, intrude on your normal working hours or affect the Ministry's reputation.

If you are planning to take on other work or services, you must talk to your manager. You will need their agreement in writing before starting.

## Staff who are also clients

If you're a staff member as well as a client of the Ministry, you must make sure anything you do as a client is honest and lawful.

It is your responsibility to give us full details about your circumstances or any changes in your circumstances to ensure you receive a correct entitlement.

# Breaches of the Code of Conduct

We need to identify breaches or potential breaches of the Code as soon as possible. We will always make sure the disciplinary process is impartial, fair, prompt and consistent. We will consider each case on its merits, including reviewing the reasons for the breach and taking into account the individual circumstances of each case before deciding on the action to take.

You can find more details of the disciplinary process on our intranet.

## Reporting breaches of the Code of Conduct

If you find out about a breach or possible breach of either the State Services Standards of Integrity and Conduct or this Code of Conduct, you should:

- think carefully about how you can deal with the situation responsibly
- discuss the issue or situation with your manager as quickly as possible – they may have additional information you might not know, so trust them to know the best way to deal with things.

Also use this process to report any breach of any other Ministry policy, procedure, standard or guideline, unless another process is provided.

If you don't think you can talk to your manager, or if the situation remains unresolved, then you can talk to another Ministry manager or the General Manager Human Resources.

If you need access to confidential counselling, the Ministry's Employee Assistance Programme (EAP) is voluntary, private, confidential and available to all Ministry staff. You can find more details on EAP on our intranet.

## Reporting serious wrongdoing

In some cases, a breach of the Code of Conduct may also be serious wrongdoing under the Protected Disclosures Act 2000. If this is the case, you can use the Ministry's Protected Disclosures procedures to report the incident or action, and receive the protections of the Act. There is information about protected disclosures on our intranet.

## If you think the Ministry has not met its obligations under the Code

If you think the Ministry has not met its obligations, follow the same process as the one to report breaches of the Code of Conduct (as set out above).

Once you have told us about your concerns, we will:

- treat your concerns confidentially, investigate them promptly and appropriately, and take action as necessary
- where appropriate, let anyone affected by an allegation know about it and ask for their explanation
- consider the use of a neutral third party to resolve the issue, if appropriate
- let you know if an investigation or action has started and stay in regular contact, if appropriate
- let you know about the outcome, where appropriate.

The Ministry will make every effort to maintain the confidentiality of an individual making a protected disclosure. This is set out in our Protected Disclosures policy.



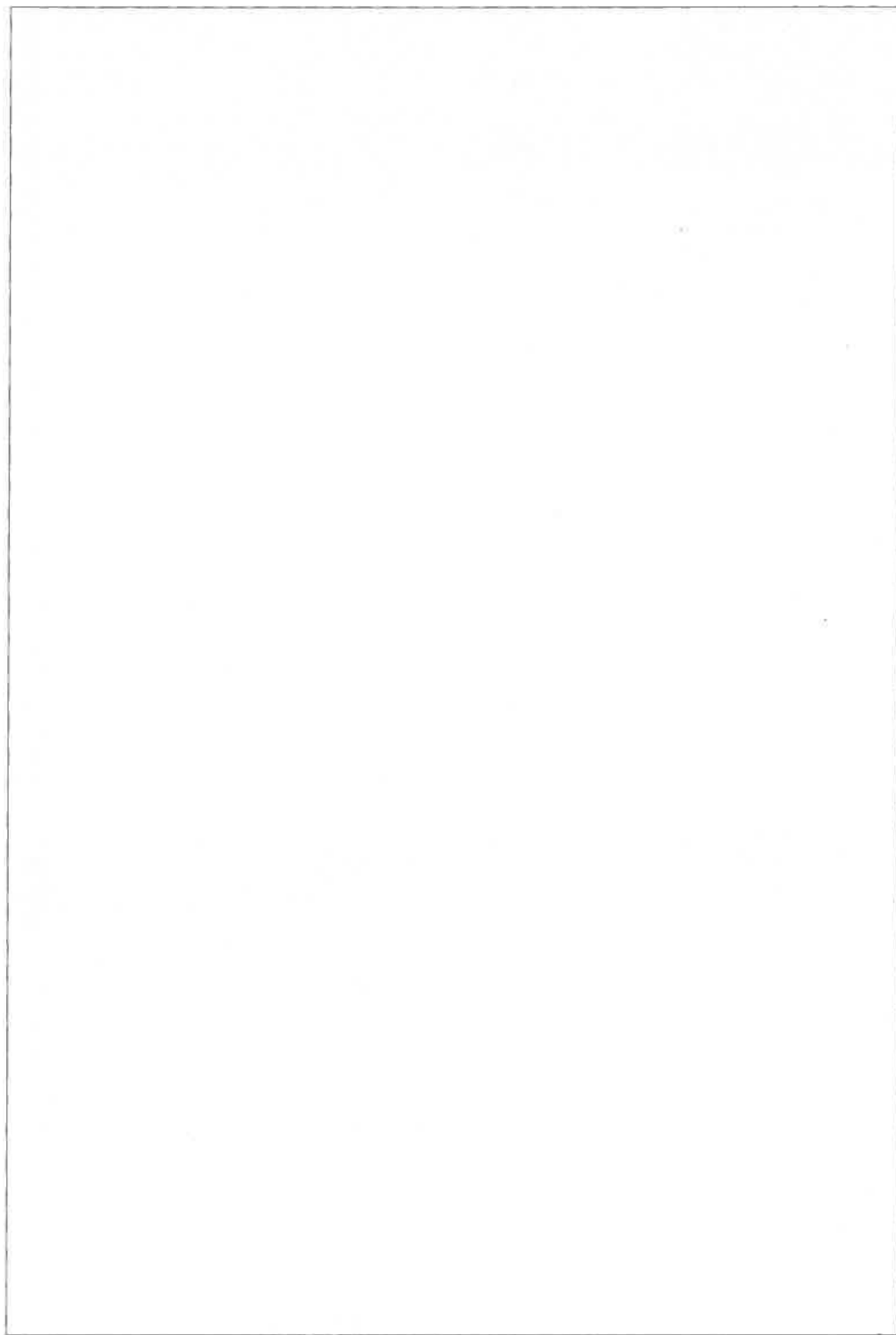
### **If you breach or think there is a risk you could breach the Code**

If you are unsure about how to deal with an ethical issue, discuss it with your manager. If your manager is involved, discuss the issue with your manager's manager or any senior manager.

Managers who are advised of a breach or a possible breach will deal with the alleged breach in accordance with the Ministry's policy. This means anyone alleging a breach or who is being investigated for a breach of the Code of Conduct will be given adequate notice of meetings, have an opportunity to be heard, and have the right to representation and/or have a support person present at meetings.

Remember, you can also face disciplinary action for breaching other Ministry policies, procedures and guidelines.

If you are unsure about how to deal with an ethical issue, discuss it with your manager. If your manager is involved, discuss the issue with your manager's manager or any senior manager.







# **MINISTRY OF SOCIAL DEVELOPMENT**

TE MANATŪ WHAKAHIATO ORA

## **MSD Social Media Policy: for the use of social media in an official capacity**

Reviewed and updated December 2020

# Table of Contents

Introduction.....	3
Purpose .....	3
Definition of social media .....	3
In scope.....	4
Not in scope .....	4
Social media help and advice.....	4
Using social media in an official capacity .....	5
Complying with the Standards of Integrity and Conduct .....	5
Complying with Political Neutrality Guidance.....	5
Following and interacting with other social media accounts .....	5
Complying with the Privacy Act.....	6
Consent should be gained from people pictured in social media posts.....	6
Protecting privacy in comments and private messages .....	6
Communicating with clients through an individual social media profile .....	6
Complying with the Public Records Act.....	7
Records Policy Statement .....	7
Assistance .....	7
Ensuring security of accounts .....	7
Requirement to publish MSD Social Media Transparency statement .....	8
Guidelines for advertising on social media .....	8
Annual review of social media account.....	8
Maintaining processes for managing risk .....	9
General guidance on responding to comments and private messages .....	9
Setting up a new MSD social media account.....	10
Process for setting up a new account.....	10
Roles and responsibilities .....	10
Communications and Engagement is responsible for: .....	10
Business groups are responsible for: .....	11
Support with social media account strategy .....	11
Risks and mitigations.....	12
Resources .....	14
Guidance for use of social media from the Public Service Commission ..	14

# **Introduction**

## **Purpose**

Social media can be an effective tool to engage with the public, and a way to listen and be responsive to their views and needs. Using social media responsibly can help to maintain the public's engagement with and trust in public services.

The purpose of this document is to provide assurance that when MSD engages in social media as a communications channel:

- MSD is represented only by authorised staff, or media/advertising agencies representing MSD
- staff have documented and approved objectives and guidelines
- risks for the organisation and individuals are mitigated
- staff are aware their responsibilities in managing the social media accounts are underpinned by the Standards of Integrity and Conduct, Political Neutrality Guidance.
- MSD's various social media presences are mandated, coordinated and overseen
- the respective roles of Communications and Engagement and business groups are clear
- existing social media expertise within MSD is leveraged
- we meet our legal obligations under the Public Records Act and the Privacy Act.

## **Definition of social media**

Broadly, 'social media' refers to internet-based tools, websites and services that allow users to interact, and create and share content. Content may take various forms - video, audio, text or multimedia. Examples of social media include blogs, microblogs, podcasts, forums, wikis, and video hosting sites.

Facebook, Twitter and LinkedIn are currently MSD's most commonly used social media channels.

Social media is a dynamic and evolving landscape, and additional forms of social media will emerge that may not be mentioned here.

## In scope

This document outlines the governance arrangements, processes and considerations for MSD staff creating or maintaining social media accounts which represent the MSD brand or sub-brands. It also includes any other social media account operated by MSD for official purposes.

The principles in this document apply to all content published on behalf of MSD using social media tools. It includes all social media accounts owned and operated by MSD, regardless of whether they are shared publicly or by invitation.

It also covers the use of social media for advertising, and the use of personal social media accounts, where they are used in an official capacity.

This document provides high-level principles for engaging in social media as a communications channel for groups in MSD who want to raise awareness and promote discussion and engagement with stakeholders and the public at large. It outlines the model for governance of social media accounts designed to mitigate risks and maximise opportunities.

## Not in scope

Staff personal social media accounts accessed during work hours are out of scope. In this context, staff should refer to information on Doogole on [Social Media Use in the Workplace](#).

The use of social media to gather information for investigations is out of scope.

## Social media help and advice

The Social Media Team in Communications and Engagement offer expertise in social media and can assist you with your queries or concerns.

Social media team		(b)(7)(D)
Lead advisor social media	(b)(7)(D)	(b)(7)(D)

## Using social media in an official capacity

These policies comply with guidance from the Public Service Commission for official use of social media.

### Complying with the Standards of Integrity and Conduct

Use of social media in an official capacity needs to be underpinned by core responsibilities under the Standards of Integrity and Conduct.

These are our responsibilities as public servants to be fair, impartial, responsible and trustworthy.

### Complying with Political Neutrality Guidance

The obligation to act in a politically neutral manner is another core responsibility in the use of social media in an official capacity. Please see Political Neutrality Guidance

Generally, a business unit should only post or share content on social media where there is a clear business purpose for doing so that is linked to the business unit's role and functions. Any content shared on social media must be:

- *Impartial and politically neutral* – this means it should be unlikely to be seen as being biased towards or as advocating for a particular political party. Careful consideration should also be given to any association with individuals, businesses and organisations.
- *Factual and accurate* – this means reasonable steps have been taken to ensure its accuracy. In particular, if a business unit is providing information about government policy, this should be factual rather than based on opinion. While public servants may publicly explain government policy, justifying or endorsing it is the role of the Minister.

### Following and interacting with other social media accounts

It's important to consider how interactions with other social media accounts could be perceived. Following another social media account, 'liking' or reposting content from another account, or linking to content from another source online is very likely to be perceived as an endorsement. Generally, this should only be done where there is a clear business purpose for doing so that is linked to your business unit's role and functions.

One option is to follow a broad range of accounts to manage any perceptions of being biased towards or as advocating a particular political party. A MSD social media account should not follow the social media accounts of individuals or organisations that are known to produce content that is offensive or questionable.

Your business unit's social media account should be judicious about 'liking' or reposting content that has been shared by other accounts. You must carefully consider whether the benefits of doing so outweigh any potential perception risks.



Your MSD social media account should frequently review your social media presence, including the other social media accounts you are following, to ensure it is current and consistent with this social media policy and with Public Service Commission guidance.

## **Complying with the Privacy Act**

### **Consent should be gained from people pictured in social media posts**

Government agencies must ensure they respect and protect people's personal information. If they are sharing any information or content on social media that relates to an identifiable individual (whether they are a member of the public or a public servant), that person must have given consent for the information to be shared.

### **Protecting privacy in comments and private messages**

There are a number of significant privacy issues that can arise in interactions with clients on social media platforms about their personal circumstances.

All information on social media is visible to the owners of those platforms, and may also be vulnerable to hacking. This includes information contained in private messages.

- No private client information should be provided on these platforms by us, including on private messages to that client.
- Clients and members of the public should be discouraged from sharing their private information with us on these platforms, including personal circumstances, client numbers, phone numbers or any other private information.
- We should also never ask them to give us personal information, either through public comments or private messages.
- If they need assistance that is particular to their circumstances, they should be redirected to other more secure channels, such as email or phone.
- Any private information that is held on private messages, and that is sent on an unsolicited basis, should be regularly removed.
- Private messaging content should be regularly archived as part of responsibilities for record keeping.

What can be helpful instead is to provide generic information when people make enquiries, or point them towards publicly available information to help them with what they need. Or direct them to other channels if they want to have a fuller conversation about their situation, eg 0800 numbers or email.

## **Communicating with clients through an individual social media profile**

Staff members must not use their personal social media accounts for client liaison – for example to get in touch with clients, make enquiries, pass on information or set up appointments. Such interactions carry a number of privacy risks, as outlined in the section above. They also blur professional and personal roles. This applies to Facebook Messenger, WhatsApp or any other social media platforms.

## **Complying with the Public Records Act**

The Public Records Act 2005 requires all public sector organisations to create and maintain records of their activities. This includes information published on social media channels, as well as private messages on those channels.

### **Records Policy Statement**

When using social media for official MSD business, staff are creating records which provide evidence of business publications, communications and activities. These records should therefore be managed throughout their life cycle in accordance with the Public Records Act, as are all other Ministry records.

All activity on MSD social media channels should be periodically captured and saved into Objective or other MSD databases. This includes content posted by MSD staff as well as private conversations with members of the public. The business owner for each social media channel is responsible for ensuring that this occurs.

The resulting record should be in a file format that is readable e.g. PDF, Excel or MS Word. The record should comprise:

- Posts / publications
- Conversations conducted in private messages

Where private messages are archived, the file titles should include:

- Name of the correspondent
- Date of the beginning of the conversation

A reference file with all names and dates should also be created, to ensure it is easy to find specific conversations. The frequency for capturing social media content will be determined by the level of activity for the particular channel and the business need it is supporting.

For example, if there has been a high level of activity the records should be captured more frequently.

### **Assistance**

Queries and requests for assistance about record keeping and social media can be directed to Information Services: [infohelp@msd.govt.nz](mailto:infohelp@msd.govt.nz)

## **Ensuring security of accounts**

All MSD social media accounts will use a password which is known only to the social media account holder(s). If possible, all MSD social media accounts should be protected with two-factor authentication (such as SMS login codes or Google Authenticator). Passwords should be changed on a regular basis.

MSD social media accounts must provide 'administrator' access to the Communication and Engagement's Social Media Team.

MSD social media accounts can be accessed from password-protected personal devices, where necessary outside of work hours. MSD social media account holders should be aware of the risk of personal material inadvertently being posted to an MSD account when MSD social media accounts are accessed on personal devices.

Where an account administrator leaves MSD or no longer has a role as an administrator for the business unit's social media account, the business unit should ensure their access to that account ends.

## **Requirement to publish MSD Social Media Transparency statement**

Each account must publish a transparency statement about their approach to using social media. This should be the MSD social media transparency statement, which can be found [here](#). It can either be published on the account profile, or the link can be provided.

The transparency statement outlines:

- how the account intends to use social media and for what purposes
- how the account will moderate comments by other people, and considerations it will use when deleting comments
- how the account will manage and respond to any private or direct messages on social media
- how members of public can raise any concerns about the account's social media use
- that by following or 'liking' content from a particular person or organisation, the account is not necessarily endorsing their views.

The MSD [transparency statement](#) can be adjusted in terms of the relevant detail for your particular account – eg your policy on responding to private messages, or in line with your policy on dealing with complaints.

MSD's social media team can provide you with any further advice on this.

## **Guidelines for advertising on social media**

Any advertising on social media needs to be consistent with the [Guidelines for Government Advertising](#).

If an agency is sharing content that could be considered to be advertising, this must also be consistent with the Guidelines.

## **Annual review of social media account**

The social media account must be formally reviewed annually to ensure it remains consistent with this policy, to evaluate if it is achieving the communication objectives outlined when the account was set up, and whether any changes in strategy or resources are needed as a result. This should be done in consultation with their usual communications advisor.

The overall social media presence should be reviewed frequently (including the other social media accounts being followed) to ensure it is current and consistent with this social media policy.

## **Maintaining processes for managing risk**

The business unit should have a clear process for assessing, identifying and managing risk on the social media account, and escalating quickly in high risk situations.

Where an issue of concern arises, advice can be sought from the business unit's communications advisor.

Where an issue is high risk, it should also be flagged with the Lead Advisor Social Media, or to the Manager, Media and Social Media where media issues may be involved. They will be able to provide advice and support.

Risk situations may include:

- concerns about the wellbeing of a client or a member of the public, as identified in comments in a post or in private messages
- a controversial post goes viral or attracts large amounts of negative comments
- serious issues are raised about an aspect of operational practice through comments or private messages
- security breaches or hacking
- threats to staff

(See also section on risks and mitigations)

## **General guidance on responding to comments and private messages**

Social media is a conversation, rather than a one-way broadcast channel. Conversations provide an opportunity to demonstrate our values in the way we engage with others.

However MSD social media account holders do not have to reply to all comments on their social media platforms, and they have the right to moderate comments and delete them if they are offensive, irrelevant, share an individual's personal information or could negatively impact perceptions of the agency's political neutrality. Policies on moderating and deleting comments are set out in the [transparency statement](#).

Note that responding to private or direct messages on a social media platform in an official capacity should be subject to the same considerations as any other official communication.

# Setting up a new MSD social media account

## Process for setting up a new account

Social media is a powerful way to engage with the public and stakeholders if it is well-managed, properly resourced and the risk landscape is navigated skilfully.

It is important that all elements of MSD's social media presence are consistent with, and linked in with, the programme of overall MSD national communications. There is an inherent reputational risk for all organisations engaging in social media.

To manage the risks, when a business group proposes to establish a new social media account, the following process is followed.

1. The proposal should be led by the business group's communications advisor. For Service Delivery regional offices, the proposal should be led by an advisor in the Service Delivery National Office communications team to ensure co-ordination with overall national communications. The Social Media Checklist on Doogle can be helpful for an initial assessment on whether a social media account is needed.
2. The social media account proposal should form part of the overall communication strategy for the programme or business group.
3. The communications strategy should include a social media strategy for the new account, outlining objectives, audience, measurements, resources and milestones. The Communications and Engagement Social Media Team can provide a template for a social media strategy on request, and can provide support and advice as needed.
4. After the proposal is approved by the business group, it should go to the Manager, Media and Social Media, and then to the GM Communications and Engagement.
5. The GM Communication and Engagement approves the strategy (or not), in consultation with the business group's usual communications advisors. In the case of a Service Delivery proposal, this would be the GM Client and Internal Communications.
6. Once the new social media profile is created, administrator access will be provided to the Communications and Engagement Social Media Team.

## Roles and responsibilities

### Communications and Engagement is responsible for:

- providing expert advice and support on social media across MSD
- supporting effective and appropriate social media use across MSD
- running MSD's Facebook, Twitter and LinkedIn

- providing an escalation point for high risk issues, to the Lead Advisor Social Media, or to the Manager, Media and Social Media where media issues may be involved
- reviewing MSD's social media policy every 12 months
- provide a backstop for accessing MSD social media accounts, in the event of an urgent situation in which the normal administrators are not available

### **Business groups are responsible for:**

- leading the communications strategy for their social media account
- day-to-day management and resourcing of their social media account, including sourcing and publishing content, and meeting costs
- ensuring privacy, security and record management guidelines are followed
- maintaining clear processes on identifying and escalating risk, and escalating and seeking advice as appropriate
- annually reviewing their social media account and transparency statement, and frequently reviewing their overall social media presence
- meeting the Standards of Integrity and Conduct and Political Neutrality Guidance with support and advice from the Social Media Team
- complying with the Privacy Act and the Public Records Act 2005, with support and advice from the MSD Information Privacy and Sharing Team.

### **Support with social media account strategy**

Communications and Engagement's Social Media Team can offer business groups advice and support as necessary to ensure that new social media accounts:

- have defined, achievable objectives
- are proposing the best platform for engagement
- have identified milestones or deliverables associated with the project
- have identified measurements of success / progress indicators
- are resourced with named staff members and agreement from their line manager
- have an identified risk owner for the social media account
- have planned processes to ensure security, and day-to-day management
- have assigned roles, responsibilities, and accountabilities (e.g. who monitors, creates content, uploads, decides what is posted, responds to comments and private messages)
- are supported with operational tools and strategic advice
- are part of, or take into account, the wider business group communications strategy
- undergo monitoring and review.



## Risks and mitigations

When a business group decides to use social media to engage with the public, they may expose themselves to some risks that are not present when engaging audiences and stakeholders using other communications channels.

Risk	Example	Mitigation
Security breaches	Social media account is hacked, and inappropriate content is posted.	Social media account managers must follow password security guidelines and keep devices secure.
Inappropriate usage	Incorrect or inappropriate content is posted by a staff member, creating reputational risk.	Clarity over who the business risk owner is.  Rapid escalation of issues where they arise.  Where appropriate, deliberate misuse handled under the Code of Conduct as an employment issue.
Ineffective or poor performance	Missed opportunities to maximise the benefits of social media.  Resources not in place to manage account.  Accounts that are set up but are unable to keep up frequency of posting or engagement.	Annual review of social media account to assess performance and progress.
Controversy develops over a post or comment	A post on the account or a comment attracts a very high degree of public interest, shares and adverse comment.	Escalation to business risk owners, and to the Lead Advisor Social Media, and/or Media and Social Media Manager.
Breach of privacy	Client information is inappropriately collected or shared through social media	To prevent this, don't take part in discussion on personal details. Move discussion to another channel. Do not encourage sharing of personal information either in

		<p>private messages or on public page.</p> <p>Regularly remove private messages from the platform and store as part of your record keeping.</p> <p>Where client information is inappropriately collected or shared, action taken will depend on the circumstances. Consult with the social media team for more advice.</p>
--	--	--