



1 July 2022

Ref: OIA 2122-2256

Shane Gibson

Email: fyi-request-19547-ab9f9bef@requests.fyi.org.nz

Tēnā koe Shane

Thank you for your email of 1 June 2022 to the Ministry of Business, Innovation and Employment (MBIE) requesting, under the Official Information Act 1982 (the Act), the following information:

"I note on your website

<https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.mbie.govt.nz%2F&data=05%7C01%7CMinisterialServices%40mbie.govt.nz%7C9ef4d71a8a8f43dac47908da434df0c5%7C78b2bd11e42b47eab0112e04c3af5ec1%7C0%7C0%7C637896299278222970%7CUnknown%7CTWFpbGZsb3d8eyJWljojMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTiI6I6k1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=XLWtF7boiHmEfPHMOU5KI7pxMruu98Pv7JRjIYbARc%3D&reserved=0> you are using Google Tag Manager and Google Analytics to record details of visits to your website.

Can you please provide the following:

- 1. The length of time this Google Analytics data is retained for.*
- 2. A copy of the Information Management policy that this data retention period is based upon."*

Our response to your request is outlined below.

Response

1. The length of time this Google Analytics data is retained for.

The website MBIE.govt.nz uses the free version of Google Universal Analytics, often referred to as GA3. It is not used to capture personally identifying information, which would be against Google's terms of service, and does not have any of GA3's advanced demographic tracking options turned on. Instructions for those who do not wish to provide any information can be found on our website's privacy page (<https://www.mbie.govt.nz/privacy/>), which also details what information is captured.

Currently, this data is retained indefinitely by Google for the purposes of historical, year on year, performance analysis. However, GA3 is currently in the process of being replaced by GA4. According to Google's roadmap ([Universal Analytics will be going away - Analytics Help \(google.com\)](https://www.google.com/analytics/docs/en/new-features/universal-analytics-will-be-going-away)), GA3 will stop capturing new data in July 2023 and existing data be only able to be accessed 'for at least six months' after that. This suggests that there will be a point after approximately 18 months whereupon all GA3 data will no longer be available to MBIE. MBIE has no plans to export that data in any format beyond the usual regular performance reports it generates for website owners and stakeholders within MBIE.

The replacement service (GA4) has a hard limit of 14 months data retention (see [Data retention - Analytics Help \(google.com\)](#)). As users of the free service, we do not expect to exceed that limit. MBIE has already begun the transition to this new service.

2. A copy of the Information Management policy that this data retention period is based upon.

In addition to our answer to Question 1 above, please find attached two documents containing MBIE's policy, procedures and guidelines on social media channels. MBIE's privacy policy has also been attached as a third document.

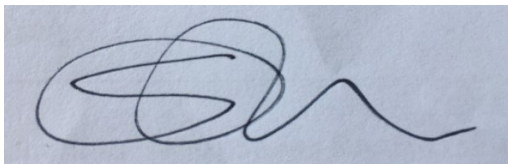
Archives New Zealand (Archives) also provides a publicly available records management schedule (General Disposal Authority 7: Facilitative, transitory, and/or short-term value records), which is relevant to your request. This permits disposal of non user generated system files, such as web analytics data, when they are no longer needed. You can find an explanation of that Authority on Archives' website here: www.archives.govt.nz/manage-information/how-to-manage-your-information/disposal/general-disposal-authorities.

The specific link to General Disposal Authority 7 is here:

assets.ctfassets.net/etfoy87fj9he/2vPln4vpuDzDatnAKz7Ccx/f7f25abf13d3fa99cfe54f07cf9d39a0/16_GDA7-General-disposal-authority-7.pdf.

We trust you find this information helpful. 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 freephone 0800 802 602.

Nāku noa, nā

A handwritten signature in black ink on a light blue background. The signature is stylized and appears to be 'Evelyn Wareham'.

Evelyn Wareham
Chief Data Officer
Digital, Data and Insights

Document schedule

Documents released

Question #	Date	Description
2	Jun 2021 (current)	MBIE Social Media Channel Policy
2	Current	MBIE Social Media Procedures and Guidelines
2	Oct 2021 (current)	MBIE Privacy Policy



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



Social Media Channel Policy

June 2021, Version 2

RELEASED UNDER THE OFFICIAL INFORMATION ACT

1 MBIE guiding principles relevant to this policy

- 1.1 The Social Media Channel policy aligns with MBIE's guiding principles of:
- a. Ensuring our core values and diverse and inclusive culture, including partnering with Māori, are at the heart of what we do
 - b. Protecting organisational reputation
 - c. Ensuring the best use of taxpayer funds
 - d. Ensuring a healthy, safe and secure environment; and
 - e. Acting with or complying with the law and legislation

2 Purpose

- 2.1 The purpose of the MBIE Social Media Channel policy is to:
- Ensure that robust processes and systems are in place for staff to manage MBIE's social media channels in a way that is consistent and appropriate
 - Help staff to engage safely and appropriately with social media to protect MBIE's security and reputation
 - Help staff to comply with NZ Government standards and charters including the [Public Service Commission Code of Conduct](#), and the [Accessibility Charter](#)

3 Scope

This policy applies to all staff, secondees and contractors, employed or engaged on any basis by the MBIE, who are authorised to use any of MBIE's social media channels for business purposes on behalf of MBIE, whether they are casual, temporary or permanent, whether full time or part time and whether they are located in New Zealand or in any other country.

The policy works alongside the [policies outlined by each social media channel](#), which must also be followed when creating a social media account.

- 3.1 For the avoidance of doubt, this policy does not cover the use of social media:
- For personal use, which is covered by the [ICT Acceptable Use Policy](#)
 - For verification and investigative purposes, which is covered by the Procedures for MBIE staff using social media for verification and investigation purposes to support regulatory compliance and law enforcement work

4 Help

- 4.1 For help with this policy contact the Principal Advisor, Design and Marketing or your account manager in the Design and Marketing team at designandmarketing@mbie.govt.nz

5 Definition of terms

Term	Definition
Social media	Websites and applications that enable users to create and share content or to participate in social networking.
Social media account	The use of a single social media channel such as Facebook or Twitter, used by MBIE.
LastPass	MBIE's approved cloud-based password management tool
Transparency Statement	A public statement that explains how you collect, use, engage and share information on social media.
Social Media Register	A secure register of every MBIE social media account, including information on management and security arrangements for each account.
Social media account holder	A person who, in the course of their employment, is authorised to create or manage an MBIE social media account and/or publishes, monitors, maintains and appropriately archives content.

6 Policy statements

6.1 MBIE recognises social media's value as a business tool to:

- Complement other integral communication and marketing channels and tools
- Increase the visibility and effectiveness of MBIE initiatives and actions
- Reach and connect with online audiences in a cost effective way
- Ensure a right-of-reply or response in online channels

Approval to set up a new account

6.2 Setting up a new social media account must be approved by General Manager ECoMS.

6.3 Every social media account must have a nominated account holder to be responsible for the day-to-day operation of the specific social media account.

6.4 The Design and Marketing team in ECoMs will maintain a secure register of every MBIE social media account.

Passwords and security

6.5 All social media accounts must apply security controls that limit administrative access to authorised account holders.

6.6 Social media accounts must maintain a high standard of password protection to prevent unauthorised use.

6.7 Passwords for all social media accounts should at minimum meet the following standards:

- a) The account password must have a minimum of 12 characters
- b) The account password must not have been used by any account administrator on any other account (work or personal)

6.8 The account password must be changed every time an authorised account administrator has access revoked.

6.9 The account password must be changed if the password is compromised.

- 6.10 All MBIE social media accounts must use two-factor authentication. Where two-factor authentication is not able to be used, passwords must be longer than the minimum requirements.
- 6.11 Only authorised staff listed in the Social Media Register can operate social media accounts on behalf of MBIE.
- 6.12 Social media account holders should manage the administration of social media accounts including managing the access to these accounts. Staff with administrative access to social media channels must have their access revoked before leaving their role. This includes staff who change roles within MBIE and who no longer require this as part of their job.
- 6.13 Authorised external agencies that have been granted administrative access to social media channels must also have this access revoked when the need for such access ends. This access can also be revoked when a dispute arises, or when circumstances deem it otherwise appropriate.

Account management

- 6.14 The GM ECoMS and/or delegates have the authority to intervene, if necessary, in any MBIE social media account or activity to protect the security or reputation of MBIE. This may be financial, operational or legal in nature and includes any information that pertains to clients and customers.
- 6.15 The GM ECoMS and/or delegates must have full administrative access of any social media account.
- 6.16 All social media accounts hosted by MBIE business units must remain politically neutral, and reasonable efforts must be made to ensure content on MBIE social media accounts is accurate and not misleading.
- 6.17 All MBIE social media accounts must have a transparency statement present on their page. This should follow the official guidance from the [Public Service Commission](#).
- 6.18 Social media account holders must exercise judgement when liking, friending or following other social media accounts or content. Staff must include a disclaimer on their page that following an account is not an endorsement of its content or of the organisation.

Privacy

- 6.19 Clear information about the [MBIE privacy policy](#) must be present in the transparency statement.
- 6.20 Personal information collected by, or sent via social media should be securely stored in the social media channel servers, as per the privacy and data policies for that channel or application (see section 10).
- 6.21 Access to personal information through the social media account will be limited to MBIE employees who have permission to access this account. Security measures must be taken to ensure MBIE social media accounts are secure from users outside of the organisation.
- 6.22 No personal information is to be collected or stored within MBIE without informed consent from the subject of the information. All reasonable steps must be taken to avoid loss, inappropriate use or disclosure of this information.
- 6.23 Any data collection through pixel or cookie tools must be clearly outlined in your website privacy policy and must give the user a chance to opt out upfront.
- 6.24 Any personal information that is collected must be disposed of once the information is no longer needed for the reasons permitted by the subject. Disposal must follow the procedure outlined in the [Records Management Policy](#).
- 6.25 The use of pixel, cookies or similar tools to collect user data must follow the MBIE Pixel Application Process (see section 8).
- 6.26 Personal information shall not be collected by unlawful or unfair means. Authorised users should be aware the use of false or fake personas is a breach of the Privacy Act 2020

- 6.27 Use of personal information in a post, link, or image must only be made with the express permission of the subject of the information, or otherwise in compliance with [MBIE's Privacy Policy](#).
- 6.28 If your role involves monitoring social media activities and you need to identify illegal activities, please contact socialmedia@mbie.govt.nz as you'll need to follow specific processes to meet New Zealand's legal and privacy requirements.

Finance

- 6.29 All social media advertising (paid or unpaid) must comply with the [Guidelines for Government Advertising](#).

Accessibility

- 6.30 Social media account holders must make a reasonable effort to ensure that content does not specifically or unintentionally discriminate against people when delivering information and services on behalf of MBIE.
- 6.31 Any [core or critical information](#) broadcast via social media should also include a link to the same information on a relevant, authoritative and fully accessible web page wherever possible.
- 6.32 Any social media content that is embedded in a website that is produced or maintained by MBIE must meet the [NZ Government Web Standards](#).

7 Key Accountabilities and Responsibilities

Role	Responsibility
Governance and Oversight	
Chief Executive (CE)	<ul style="list-style-type: none"> Accountable for MBIE meeting its obligations under this policy
Organisational Capability and Assurance Committee (OrCA)	<ul style="list-style-type: none"> Maintaining overall oversight of this policy Approving major changes to this policy and associated procedures
DCE Sponsor	<ul style="list-style-type: none"> Approving minor changes to the policy and associated procedures Endorsing major changes to this policy Ensuring awareness of this this policy across MBIE
Business Groups: Identify and manage risks in day-to-day operations (1st Line)	
DCEs	<ul style="list-style-type: none"> Embedding this policy in their business groups
All Managers	<ul style="list-style-type: none"> Embedding this policy and associated procedures into their business activities Monitoring compliance with this policy and procedures in their business area and reporting any non-compliance to the policy owner Ensuring new and existing staff in their teams are made aware of and comply with this policy and procedures
Social Media Account Holders	<ul style="list-style-type: none"> Ensuring that administrative access to social media channels be revoked when the need for such access ends Providing discretionary access when circumstances deem it appropriate

	<ul style="list-style-type: none"> • Ensuring social media accounts are appropriately monitored and moderated, and issues are identified and escalated as required • Ensuring compliance reporting is provided to the policy owner, on a quarterly basis and as required • Updating and maintaining social media accounts, including managing access to accounts and ensuring passwords are kept secure • Monitoring and moderating content published by users and followers • Reporting comments/posts that may impact on MBIE security or reputation to Engagement and Communications Manager, and/or Design and Marketing team • Ensuring appropriate record management is in place, including for personal information and public records • Ensuring suitable continuity of social media accounts, and closing accounts when they are no longer required • Ensuring complaints or negative queries about MBIE’s social media use are dealt with appropriately • Ensuring they have the appropriate approval to share/post content e.g. permission to use or disclose personal information, and/or material protected by intellectual property rights, including images • Ensuring that the use of the information is the use for which it was intended upon collection and is the use for which we have consent (e.g., was disclosed in the privacy statement at the time of collection) • Ensuring content posted to social media accounts meets accessibility requirements • Providing compliance reporting information to the Principal Advisor, Design and Marketing on a quarterly basis, and as required
--	--

Risk Oversight Functions: Setting policies and monitoring compliance (2nd Line)

<p>General Manager, ECoMS (Policy Owner)</p>	<ul style="list-style-type: none"> • Undertaking appropriate co-design and consultation when developing / reviewing policies • Ensuring suitable communication, training and guidance is provided to business groups to embed policies and procedures into operational activities • Providing advice and support to business groups relating to this policy and procedures • Assisting business group with any breach management / mitigation activities as required • Monitoring compliance with this policy and procedures on a regular basis • Ensuring the policies and procedures are reviewed and updated as relevant or by the agreed review date • Providing quarterly reporting on policy compliance to Enterprise Risk and Compliance
---	--

Design and Marketing Team	<ul style="list-style-type: none"> • Providing advice and recommendations to account holders, teams/business units as per the policy and procedures, in consultation with the Principal Marketing Advisor • Collecting compliance information from social media account holders on a quarterly basis, and as required. • Monitoring MBIE's social media presence • Carrying out periodic reviews of a random sample of MBIE social media accounts • Recommending business cases for new social media accounts before final approval received by GM ECoMS • Promoting awareness of and compliance with this policy • Promoting best practice • Providing assurance to the Policy Owner that advice and recommendations provided to MBIE are in line with this Policy and related procedures
----------------------------------	--

8 Procedures

8.1 [Social Media Procedures and Guidelines](#)

8.2 [MBIE Pixel Application Process](#)

9 Related MBIE policies and documents

Legislation	Relevance
ICT Acceptable Use Policy	Covers personal use of social media accounts by MBIE employees
Process for using social media for investigation purposes	Covers use of social media for investigation purposes
News Media Policy	Outlines how to process news media requests that may be received via social media accounts
Code of Conduct	Sets the expected behaviour of all MBIE staff and how they must engage with the public on social media
Privacy Policy	Ensures that appropriate processes, procedures and systems are in place to manage personal information that may be received through social media
Records Management Policy	Ensures client or sensitive information received through social media is protected from unauthorised access
Protective Security Policy	Outlines how to provide a safe and secure environment for our people, information and assets

10 Other related policies and documents

Legislation	Relevance
Facebook and Instagram Terms of Service	Outlines the terms of use that Facebook and Instagram require from account holders

Legislation	Relevance
Twitter Terms of Service	Outlines the terms of use that Twitter requires from account holders
LinkedIn User Agreement	Outlines the terms of use that LinkedIn requires from account holders
YouTube Terms of Service	Outlines the terms of use that YouTube requires from account holders

11 Relevant legislation, regulations and standards

Legislation	Relevance
Copyright Act 1994	Outlines use of copyrighted material in NZ, including imagery
Official Information Act 1982	Outlines the law around requesting information through the Official Information Act – which can be done through social media
Privacy Act 2020	Outlines the law around the use of personal information
Harmful Digital Communications Act 2015	Ensures there is no harm caused to individuals by digital communications

12 Measures of success and compliance management

12.1 The General Manager ECoMS will assess the effectiveness and compliance with this policy. The following measures of success outline what we expect to see if the policy is working:

- a. Content and responses of social media accounts are appropriate, uphold the reputation of MBIE and meets NZ Government Web Accessibility & Usability Standards where applicable
- b. Social media accounts are operated only by authorised staff
- c. All new social media accounts have followed the correct approval process

The General Manager ECoMS will monitor compliance with this policy as follows:

- Training provided to account holders by the Design and Marketing team to support appropriate awareness and understanding of social media procedures
- The central social media account register which lists authorised account holders, a record of breaches and remedial actions taken to comply with the Policy
- Random review of social media accounts for compliance with this policy
- The use of tools (such as Sprout social) and the procedure and guideline documents for meeting social media content requirements

12.2 These processes help ensure compliance with this policy and related mandatory procedures, as well as identifying risks so they can be managed appropriately.

Compliance information regarding the performance of this policy will be provided to the Enterprise Risk and Compliance branch of Finance and Performance on a quarterly basis.

13 Non-compliance

13.1 Failure to comply with this policy may be considered a breach of the Code of Conduct.



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



Social Media Procedures and Guidelines

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Contents

Purpose	3
Scope	3
Government guidelines	3
Social media procedures	4
Creating an account	4
Channel security	4
Passwords	4
Staff access	4
Other security measures	5
Privacy	5
Transparency statement (Terms of use)	5
Pixel Application Process	5
Working with external agencies	6
Social media guidelines	7
Channel content	7
Approval processes	7
Risk mitigation	7
Political neutrality	7
Accessibility	7
Sharing external content	8
Working with influencers	8
Monitoring	8
Official information act and privacy requests	9
Responding to media queries	9
Reporting	9
Help and resources	9

Purpose

These procedures and guidelines are for everyone who uses social media channels on behalf of MBIE. They should be read and understood in conjunction with the [Social Media Channel Policy](#) and the [State Sector Code of Conduct](#).

Our vision is that MBIE social media channels are:

- Trusted as a reputable source of information
- Recognised as leaders in best practice across Government
- Underpinned by MBIE values
- Contributing to our mission to Grow New Zealand for All
- Aligned with our wider communications strategies

Scope

These procedures and guidelines apply to all MBIE teams who are authorised to use social media channels. They will be adjusted as new practices arise.

Examples of social media channels used within MBIE include:

- Facebook
- LinkedIn
- Twitter
- Instagram
- YouTube

Government guidelines

The State Services Commission has produced [Guidance for State Services Official use of Social Media](#). Other government policies and procedures may also apply, including but not limited to:

- [Guidelines for Government Advertising](#)
- [Political Neutrality Guidance](#)

Social media procedures

Outlines the procedures that all social media account holders must follow when creating and managing an MBIE social media account, as per the Social Media Channel Policy.

Creating an account

It's important to think about how social media fits into your overall communication and/or engagement strategy and to have a clear purpose for choosing it as a channel.

In order to create a new social media account, you will need to create a business case that outlines why a social media channel would benefit your objectives.

The business case must be developed in consultation with the Design and Marketing team and be approved by the business units Communications Manager and General Manager. Final approval of the business case will be by the General Manager ECoMS.

Key items to cover in your business case include:

- Your intended purpose, benefits and audience needs
- How you will resource the channel (i.e content creation, moderation, DMs). This takes at least 6-8 hours per week.
- Any potential or real risks and how you will mitigate these
- A clear channel strategy – who you are targeting, what you hope to achieve etc
- A draft content plan, including examples of the kind of content you will post

All accounts must be added to the social media register, held by the Design and Marketing team. This should include a list of the nominated account holders. These account holders are the only people who are allowed to use social media on behalf of MBIE.

Administration access to social media accounts must also be granted to the Design and Marketing team.

Channel security

It's important that the public facing channels are managed securely. All social media channels must follow the security requirements below.

Passwords

Passwords for all social media accounts should at minimum meet the following standards:

- The account password must have a minimum of 12 characters.
- The account password must not have been used by any account administrator on any other account (work or personal).

The account password can be stored by account administrators, but it must be encrypted. This means passwords can be stored in a password manager (such as MBIE's LastPass account), but cannot be stored in plain text (e.g. they cannot be stored on the intranet or in a spreadsheet or document).

Staff access

Staff with administrative access to social media channels must have their access revoked by their team's social media channel admin before their off-boarding process can be completed. This includes staff who change roles within MBIE and who no longer require this as part of their job.

The Design and Marketing team must be notified when there is a change in administrative access to your account so that the social media register can be updated.

Other security measures

All staff with access to an MBIE social media account must turn on two-factor authentication. This can be turned on in the account's security and privacy settings.

If you have to step away from your device, lock it and make sure it requires a strong password to unlock – even if you're at home.

If your corporate social media account is breached, report it to the Design and Marketing team, MBIE Security team and CERT NZ straight way for help and advice.

Privacy

Personal information collected by social media should be securely stored in the social media channel servers. No personal information is to be collected or stored within MBIE without informed consent from the subject of the information.

If you need to share information, let the user know, or completely redact any personal information. This must then be disposed of once no longer needed.

Use of personal information in a post, link, or image must only be made with the express permission of the subject of the information.

Transparency statement (Terms of use)

State Sector policy requires that agencies must publish a transparency statement about their approach to using social media in a place where it is easily accessible for members of the public (eg on their websites and/or official social media channels).

The transparency statement should clearly outline:

- The [MBIE privacy policy](#)
- How you intend to use social media and for what purposes
- How you will moderate comments by other people, and considerations you will use when deleting comments
- How you will manage and respond to any private or direct messages on social media
- How members of the public can raise any concerns about the agency's social media use and;
- That following or 'liking' content from a particular person or organisation, is not necessarily endorsing their views.

When setting up your social media account you can use the [MBIE Social Media Terms of Use](#) or you can create your own.

Pixel Application Process

If you have a team who would like to add a social media pixel to their social media account, they will need to complete a [Pixel Application Form](#).

In this form they will need to:

1. Demonstrate how the use of this tool fits in with your wider strategy
2. Complete a [Privacy Impact Assessment](#) with the MBIE Privacy team
3. Update your website's Privacy page to include the use of Pixel

4. Engage with the Digital Tools team (different to the Digital Channels team, Digital Tools helps with adding pixels and creating pop up banners) to let them know your intention to implement this tool and to organise an opt-in option
5. Send to the legal team for approval

Once you have completed the Pixel application form, it needs to be reviewed by someone in the Design and Marketing team and then approved by the business group General Manager.

Any data collection through pixel or cookie tools must be clearly outlined in your website privacy policy and must give the user a chance to opt out upfront.

Note that social media accounts that sit within the Te Whakatairanga Service Delivery Group will need to confirm their pixel process with the CXI team.

Working with external agencies

Agencies may be granted restricted access to MBIE social media ad accounts for the purposes of managing campaign content or advertising. Note that this restricted access should include creating and managing ads, but not admin access to the ad account.

It is your responsibility to ensure the external agency understands their obligations, is contracted using the correct procurement process and has their access revoked on completion of the contract. If you have any questions, please contact your Design and Marketing Team Account Manager.

Social media guidelines

Key guidelines that all social media account holders should follow to maintain best practice when running a social media account.

Channel content

The public looks to government as a credible, reputable source of truth. Our content should always be relevant, factual, friendly and politically neutral.

Approval processes

Teams with a social media account must have a clear content plan and approval process in place for each channel.

This should include a documented approval process for drafting, reviewing and approving content, as well as scheduling and posting.

Best practice is to also have a content calendar that can be used as a central content source.

Risk mitigation

As social media is a public forum, there can be a high level of risk when posting content. You should always consider:

1. Context: What is your intent for this content and are there any risks associated with posting the content?
2. Timing: Are there any other announcements happening in the near future that may impact what is being communicated?
3. Resourcing: Does the content have the potential to increase incoming calls, messages or media enquiries?

During political or high risk environments, social media posts should be re-reviewed more frequently depending on the current landscape e.g. elections, COVID-19.

You can find further advice for [managing social media during an emergency situation](#) on Te Taura.

Political neutrality

MBIE staff, and agencies acting on behalf of MBIE, are required to act in a politically neutral manner.

In order to ensure you remain politically neutral you must:

- Always remain fair and impartial
- Ensure that there is no potential bias towards one political party or view
- Include all relevant information about a topic in a factual manner

It is our role to publically explain government policy. Defending or justifying it is the role of the Minister.

Accessibility

MBIE is committed to the [Accessibility Charter](#) which includes meeting the [NZ Government Web Standards](#) and ensuring all forms of communication, including social media, are available in a range of accessible formats.

All social media content must be compliant with accessibility standards. This means:

- Providing closed captions for all pre-recorded audio and video content.
- Providing alternatives to your content that give equivalent information i.e. a transcript for pre-recorded audio, or an audio track for pre-recorded video
- Use descriptive captions to describe what you are sharing
- If multiple languages are needed, ensure that bilingual closed captions are added

Outside of including captions and descriptions, social media content should also:

- Use plain language and avoid acronyms
- Capitalise the first letter of each word in a hashtag
- Be mindful of cultural sensitivities, particularly when selecting imagery
- Ensure gender balance in roles of authority or domestic settings
- Reflect the diverse communities we serve

Sharing external content

External content can be shared on your social media account, but you must ensure that the content is:

- From legitimate sources only, such as government websites
- Impartial and politically neutral. Not advocating for a particular political party, group, individual, business or organisation
- Factual and accurate, not based on opinion

When sharing content you should always include a comment to express your business unit's involvement and why this is relevant to your content strategy.

Note that sharing content may be seen as Government endorsement, so think carefully before linking to private organisations, lobby groups and industry organisations. The default position should be not to promote commercial organisations. Exceptions to this must be for legitimate business reasons, such as a partnership with the organisation.

Linking to news articles should be done with care, as these are often based on opinion.

Reasons for linking to news articles could include; promoting an article about your organisation or building credibility due to the positive content in the article

Working with influencers

If you are considering using social media influencers always discuss this with your Communications team first, and:

- Make sure you are aware of best practice in New Zealand including [Advertising Standards Authority](#) guidelines
- Research any prospective influencers and their existing and previous brand relationships
- Be clear on who owns the content created as part of your agreement and who will control the copy/content they produce on your behalf
- Make sure they use express identifiers like #ad or #sponsored

See our [Social Media Best Practice Guides](#) on Te Taura for more information on creating good social media posts.

Monitoring

Each account should have a dedicated account manager who is responsible for monitoring and a documented process for responding to customers.

All social media account managers should monitor their channels daily and respond to queries in a timely fashion.

Key things to include in your process include:

- Always report and remove any content that breaches our terms of use
- Respond to questions about MBIE related issues where possible – note that our policy is to link to the correct webpage or contact page for more information where possible
- Have a plan to escalate negative comments and messages
- If you need to send the post on for more information internally, then always ensure all personal information is redacted

The [MBIE response framework](#) can offer more guidance on responding to social media queries.

You can also find more information on dealing with abusive comments in the [MBIE approach to abusive comments on Social Media](#).

Official information act and privacy requests

Under the Official Information Act 1982 requests can be made through any communications channel, this includes social media. People may also request personal information via social media.

Email uia@mbie.govt.nz if you receive an OIA request through social media.

If it's not possible to provide the requested information through the same channel that the request was made, ask for an email or postal address to deliver the information.

We are required to respond to OIA requests within 20 working days.

Responding to media queries

The [News Media Policy](#) and [Media Guidelines](#) cover responses to enquiries through social media. If a query is made by a journalist via an MBIE social media account they should be referred to the MBIE Communications team on 027 442 2141 or email media@mbie.govt.nz

Reporting

Reporting on the social media policy is conducted quarterly by the Design and Marketing team. This is then sent on to the policy team and policy owners to prove that we are staying compliant with the policy.

All social media account holders within MBIE need to report on their activity as part of their agreement to hold an account. This includes:

- Authorised access and any changes in account access requirements
- Issues where escalation has been required

The Design and Marketing team will send you a report template to complete and return for each of your social media channels. This is then recorded in the MBIE social media register.

Help and resources

You can find a range of support resources on our [Social Media page](#) on Te Taura.

For further guidance and advice on using social media, please contact the Design and Marketing team.



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



Privacy Policy

Version 4.1 October 2021

RELEASED UNDER THE OFFICIAL INFORMATION ACT

1. MBIE guiding principles relevant to this policy

1.1 The following MBIE guiding principles are relevant to the Privacy Policy:

- a. ensuring our core values and diverse and inclusive culture, including partnering with Māori, are at the heart of what we do
- b. protecting organisational reputation
- c. ensuring a healthy, safe and secure environment
- d. being a good employer
- e. acting with or complying with the law and legislation.

1.2 Ensuring appropriate care, respect, and controls are considered when handling the personal information in our care is key to MBIE's overall objective to Grow New Zealand for All: **Hikina Whakatutuki**

1.3 The values and behaviours that are core to this Policy are:

a. **Pae Kahurangi: We protect what's precious, our taonga**

Respectful handling of the personal information in our care is key to demonstrating MBIE's value of retaining and building trust and confidence to enable us to build our future.

b. **Māia: We explore new ideas**

Assessing risks to individual privacy when developing or adopting new processes, systems and technologies will ensure our new initiatives are respectful of people's rights, comply with relevant legislation, and have the right protections in place to minimise the risk of something going wrong.

2. Purpose

2.1 The purpose of this Policy is to ensure:

- a. that appropriate policies, processes, procedures and systems are in place to manage personal information in line with government, public, and individual expectations, and to protect the privacy of individuals
- b. the legitimate and safe use of the personal information, including personal information about MBIE people, we hold to enable MBIE to improve productivity and business performance, in order to Grow New Zealand for All.

3. Scope

3.1 This Policy applies to all:

- a. staff, secondees and contractors, employed or engaged on any basis by MBIE, whether they are casual, temporary or permanent, whether full time or part time and whether they are located in New Zealand or in any other country
- b. personal information that MBIE collects, uses, accesses, shares, stores and disposes of.

4. Help

4.1 For any queries related to this policy, please contact the Privacy Team at privacyteam@mbie.govt.nz.

5. Definition of terms

Term	Definition
MBIE people	All staff, secondees and contractors, employed or engaged on any basis by MBIE, whether they are casual, temporary or permanent, whether full time or part time and whether they are located in New Zealand or in any other country, and who have access to any personal information MBIE holds.
Privacy event	Where MBIE (including our contractors and third party service providers) fails to manage personal information in accordance with the Privacy Act or MBIE's Privacy Policy, processes and standards. It includes all privacy breaches (where personal information is wrongly collected, used, accessed, disclosed, kept or withheld as set out by the Privacy Act 2020) and potential privacy breaches ('near misses') (where an action could have resulted in a breach, but the breach does not occur).
Personal information	Any information about an identifiable individual.

6. Policy statements

- 6.1 MBIE will demonstrate the appropriate standards of care and respect required to ensure that individuals trust us with their personal information.
- 6.2 MBIE will be open and transparent about how we collect, use, access, share, store and dispose of the personal information in our care. We will ensure that our data collection (particularly from children and young people), use and sharing is lawful. We will use explicit informed consent wherever possible, to achieve our capability priority of being empowered by data while protecting the privacy and data sovereignty of individuals.
- 6.3 MBIE will maximise the value of the personal information we hold to deliver better public services and improved economic outcomes for New Zealanders.
- 6.4 MBIE will make the personal information we hold available externally to the maximum extent permissible lawfully to deliver better public services and improved economic outcomes for New Zealanders.
- 6.5 MBIE will promote innovation by combining personal information from internal and external sources, using and sharing this as appropriate, to increase our efficiency and effectiveness.
- 6.6 MBIE will foster a culture of continuous improvement by having a consistent approach for managing privacy-related business activities, compliance monitoring, performance measures and event management, and by sharing experiences, failures, successes and best practices.
- 6.7 MBIE will ensure people are comfortable coming forward to report privacy events that result from an honest mistake, through correct channels and as soon as practicable. This is in line with three of our core values: Pono me te Tika, Mahi Tahi and Pae Kahurangi. People will be encouraged to take responsibility and to commit to doing things right. Reporting near misses or actual privacy events means we can share our knowledge and learn from the past to shape the future.

7. Key Accountabilities and Responsibilities

Role	Responsibility
Governance and Oversight	
Chief Executive	<ul style="list-style-type: none"> Approves major amendments to this Policy Ensures MBIE meets its obligations under this Policy
Organisational Capability and Assurance Committee	<ul style="list-style-type: none"> Reviews and endorses major amendments to this Policy and or recommending changes to the Policy Provides strategic direction and leadership to ensure MBIE operates a safe and secure environment for our people, customers and information
Deputy Secretary, Ngā Pou o te Taumarau	<ul style="list-style-type: none"> approves minor amendments to this Policy
Business Groups: Identify and manage risks in day-to-day operations (1st line)	
All Deputy Secretaries	<ul style="list-style-type: none"> Embed this Policy and associated Procedures in their groups Ensure privacy risks are appropriately assessed and captured in the business group and branch risk registers Ensure their business groups are compliant with this Policy and have appropriate monitoring and reporting in place, including raising issues and reporting events Alert the Policy Owner to new areas of functions with their business group that collect and use personal information
Managers	<ul style="list-style-type: none"> Use personal information legitimately and safely to deliver MBIE's services efficiently and effectively Promote innovation by combining personal information from internal and external sources, using and sharing this as appropriate to improve the quality and performance of MBIE's services Ensure Privacy Threshold and Privacy Impact Assessments are completed creating new or changing existing systems and processes Reinforce MBIE's commitment to use and share personal information, proactively managing their area of accountability to ensure appropriate privacy measures are in place Ensure MBIE people are appropriately trained on how to handle personal information, including raising issues and reporting events Ensure all legal requirements and MBIE-wide policies are complied with when personal information is used and shared within MBIE or other organisations
All MBIE People	<ul style="list-style-type: none"> Comply with this and all other relevant MBIE policies

Role	Responsibility
	<ul style="list-style-type: none"> • Complete mandatory Privacy training • Manage personal information in accordance with MBIE policies, processes and systems, and practices • Maintain the integrity, accuracy and confidentiality of personal information they deal with • Respond to requests for access, withdrawal of consent and correction made by individuals • Identify privacy issues and events and report these to their manager
Risk Oversight Functions: Setting policies and monitoring compliance (2nd Line)	
Chief Privacy Officer (Policy Owner)	<ul style="list-style-type: none"> • Ensures appropriate and thorough incident management in the event of a significant privacy breach • Ensures the Policy is working effectively through regular monitoring and reporting of compliance on the Policy • Responsible for MBIE's relationships with the Government Chief Privacy Officer and the Privacy Commissioner
Legal Team	<ul style="list-style-type: none"> • Provides privacy legal advice, including on information sharing, events, complaints, and on requests for personal information, including grounds for withholding information
Privacy Advisory Group	<ul style="list-style-type: none"> • Provides functional leadership for strategic privacy matters • Drives the creation of a culture that sets the tone for respect for privacy
Privacy Team	<ul style="list-style-type: none"> • Leads the development, promotion, and embedding of MBIE's privacy capability and culture, including training, education and awareness • Provides support, advice, guidance, training on privacy considerations, legislative requirements, and best practice across MBIE • Reviews Privacy Threshold and Impact Assessments including providing advice and recommendations around related privacy risks and mitigations • Supports the management of privacy events, complaints and requests with advice and recommendations • Provides an organisational view of privacy at MBIE, including trend reporting and insights around reported privacy events, complaints, and completed Privacy Threshold and Impact Assessments, and privacy training completions
Business Change Owners	<ul style="list-style-type: none"> • Ensure Privacy Impact Assessment Framework is applied to their projects, including ensuring completion of Privacy Threshold Assessments as required • Approve and sign off Privacy Threshold Assessments (and Privacy Impact Assessments, if required), apply any

Role	Responsibility
	practicable Privacy Team recommendations and accept and sign off any privacy risk associated with the projects under their responsibility

8. Procedures

- a. [Personal information collection](#)
- b. [Personal information requests](#)
- c. [Personal information correction](#)
- d. [Complaints](#)
- e. [Privacy events](#)
- f. [Third party arrangements](#)
- g. [Privacy Impact Assessments](#)
- h. [Staff personal information security standard](#)

9. Related MBIE policies and documents

- a. [Code of Conduct](#)
- b. [Compliance Policy](#)
- c. [Protective Security Policy](#)
- d. [Records Management Policy](#)
- e. [ICT Acceptable Use Policy](#)
- f. [Risk Management Policy](#)
- g. [Official Information Act Requests Policy](#)
- h. [Social Media Policy](#)
- i. [Data merging framework](#)
- j. [Inter-agency data sharing framework](#)
- k. [Intra-agency data sharing framework](#) Information Gathering Policy
- l. [Model Standards for Information Gathering](#)

10. Relevant legislation and regulations

- a. Privacy Act 2020
- b. Official Information Act 1982
- c. Public Records Act 2005

11. Measures of success and compliance management

11.1 The Chief Privacy Officers will monitor the success of this Policy. The following measures of success outline what we expect to see if the Policy is working:

- a. An increase in privacy maturity, as rated by the annual Privacy Maturity Assessment Framework self-assessment and report to the GCPO
- b. An increase in trustworthiness, as measured by the annual Privacy Survey
- c. A reduction in harm, as measured by a decrease in reported customer complaints and negative findings.

- 11.2 The Chief Privacy Officer will monitor compliance with the Policy as follows:
- a. Availability of procedures and guidance issued under this Policy on Te Taura and ensuring these are kept up to date for any changes to legislation and regulations
 - b. Completion of mandatory privacy training
 - c. Completion of Privacy Threshold and Impact Assessments
 - d. Event reporting, including root cause analysis of privacy events report to assess the effectiveness of the Policy and provide feedback and recommendations to the relevant business groups to strengthen internal processes and to comply with this Policy.
- 11.3 Compliance information regarding the performance of this policy will be provided to the relevant business group and the Enterprise Risk and Compliance branch on a quarterly basis.

12. Non-compliance

- 12.1 Failure to comply with this policy may be considered a breach of the Code of Conduct.