MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

28 September 2023

Tēnā koe

On 31 August 2023, you requested, via the FYI website, under the Official Information Act 1982 (the Act) the following information from the Ministry of Social Development (the Ministry):

1. *Copies of the Ministry's policies, procedures, and processes regarding the use of teams by staff members, including requests to access teams chats by managers.*

2. *How many requests for access to staff members' teams chats have been made by managers and/or people leaders in the past 12 months? What justifications or reasons are required when lodging a request to access staff members' teams records? Are the staff members advised when these requests are lodged as part of the process? Is privacy a factor considered when deciding whether to grant access?*

The Ministry has interpreted your request to be for information regarding appropriate use of Microsoft Teams by staff, rather than operational or 'how-to' guidance. Please contact the Ministry is this was not the intent of your request.

I will now respond to your questions in turn.

1. *Copies of the Ministry's policies, procedures, and processes regarding the use of teams by staff members, including requests to access teams chats by managers.*

Our use of Microsoft Teams by Ministry staff is covered by both the Ministry's overarching policies for information and technology by using Microsoft Teams specific guidance and processes.

Please find attached the following documents:

- Information Governance Policy, reviewed October 2022.
- Recording Standard, approved 13 April 2022.
- MSD Survey Standard, approved 15 June 2022.

- SharePoint page - Personal information use scenarios.
- SharePoint page - Where does information belong?
- SharePoint page - Microsoft Teams Terms of Use.

Two additional documents were also identified to contain information partially in scope of your request. To expedite a response to you, the relevant sections of these documents have been provided as excerpts in accordance with section 16(1)(e) of the Act. You will find the excerpted sections of the following documents in the **Appendix**:

- Ministry of Social Development Information Security Policies – Acceptable Use of Technology Policy, approved 28 March 2017.
- SharePoint page - Recording Meetings with Microsoft Teams (National Office and Whaikaha).

You will note some additional guidelines are referenced in the Acceptable Use of Technology Policy. However, the Ministry does not believe these are in scope of your request and as such, we have not included copies of them in this response.

2. *How many requests for access to staff members' teams chats have been made by managers and/or people leaders in the past 12 months? What justifications or reasons are required when lodging a request to access staff members' teams records? Are the staff members advised when these requests are lodged as part of the process? Is privacy a factor considered when deciding whether to grant access?*

The Ministry's Internal Integrity team have not received any requests by managers to access staff member's Teams chats in the past 12 months.

In order to make a request to Internal Integrity to access Teams chat data, there must be cause for suspicion of inappropriate behaviour by the staff member. For example, this could include suspicion of fraud, corruption, misappropriation or dishonesty. Staff are not advised of any requests that are made unless the investigation results in detection of serious misconduct, in which case the staff member, their manager and Human Resources will be advised of the outcome.

Additionally, requests to access Teams chats can be made as part of OIA or Privacy Act requests. Any information of this nature will be managed securely by the appropriate team and assessed under the grounds of the respective Act. These requests may be made to other business units at the Ministry (such as the Windows and Integration team), and requests of this nature are not centrally recorded. In order to find the total number of Ministry-wide requests for Teams chats made by managers or people leaders in the last 12 months, the Ministry would need to divert personnel from their core duties and allocate extra time to manually review a significant number of files.

The diversion of these resources would impair the Ministry's ability to continue standard operations and would be an inefficient use of the Ministry's resources. As such, your request is refused under section 18(f) of the Act as it requires substantial collation. The greater public interest is in the effective and efficient administration of the public service.

I have considered whether the Ministry would be able to respond to your requests given extra time, or the ability to charge for the information requested. I have concluded that, in either case, the Ministry's ability to undertake its work would still be prejudiced.

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

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

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

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

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

Ngā mihi nui

Fiona McElwee
Director
Information Foundations

Information Governance Policy

Last Review Date:	October 2022
Next Review Date:	October 2024
Approved by:	Organisational Health Committee
Owner:	General Manager Information

Purpose

This policy defines the principles, roles, and responsibilities which support the Ministry of Social Development (the Ministry) in upholding its Information Governance responsibilities to the New Zealand Government and public. The principles found in this policy set the governing direction and intent for Information Governance. Underpinning this policy are standards, patterns, processes, and guidance material which collectively operationalise the principles in this policy and align the Ministry's Information culture and decision-making.

Policy Statement

The Ministry holds and uses information and data about people that impacts their lives. Information is taonga, and as its stewards we must both use it responsibly and protect it while it is in our care.

Effective information governance requires the Ministry to understand the information it holds, define who is responsible for that information, and know how that information is being used. Additionally, it requires the Ministry to have assurance that its information is protected, is managed appropriately, and its staff are acting responsibly when using information.

Scope

This policy applies to all Ministry staff including contractors; all information and data held and used by the Ministry; and all activity conducted by third parties on behalf of the Ministry.

RELEASED UNDER THE OFFICIAL INFORMATION ACT
Approved by Organisational Health

Policy principles

The following principles must be understood and followed to ensure alignment with the purpose of this policy.

1. The Ministry's information assets are identified and appropriately protected based on legislative requirements, information value and risk culture

The Ministry manages information assets in accordance with legislative requirements defined in the Public Records Act 2005, Privacy Act 2020, the Protective Security Requirements (PSR) and the Official Information Act (1982). The Ministry's standards define the measures which set the baseline for how information assets are secured, stored, used, and managed using a risk-based approach.

2. All information assets held by the Ministry have responsible owners to ensure they are managed appropriately

An information asset has value to the Ministry from the point of creation or collection through to eventual disposal. Information asset owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored throughout the lifecycle. Any legal and regulatory requirements applicable to the collection, storage and use of the information must be understood by the information asset owner.

3. Information assets are fit-for-purpose to promote informed decision-making

Consistently and continuously maintaining the integrity of Ministry information assets ensures people use authoritative information. The information collected, used, and shared by the Ministry is appropriate for the purpose it is intended and collected for, and contributes towards better insights, better decisions, and better lives.

4. The Ministry partners with tangata whenua in decision-making about information held by MSD to support Māori

The Ministry invests in trusted partnerships with Māori and ensures it embeds the needs of Māori in the ways it protects, stores, uses, and maintains Māori data and information. The Ministry recognises Māori data as taonga and manages it as such. In acknowledging its Te Tiriti o Waitangi responsibilities, the Ministry is committed to partnering with Māori in decisions made to govern Māori data and information assets.

5. The protection and responsible use of Ministry information is everyone's responsibility

Ministry staff are responsible for handling Ministry-held information and data appropriately. While Ministry technology and processes play a key role in providing a layer of protection over information, our awareness of information risk and its acceptable use is just as important. The Ministry expects staff to act in a timely and coordinated manner to prevent or respond to breaches of, and threats to, information.

RELEASED UNDER THE OFFICIAL INFORMATION ACT
Approved by Ministerial Governance Committee October 2022

Roles and Responsibilities

Everyone that works for or is contracted to the Ministry has a responsibility to comply with this policy. The responsibility of each role specifically relevant to this policy is set out in the table below:

Person/Party	Responsibility
All Staff	All staff are responsible for: • Complying with the Ministry's information policies • Following information guidance and training • Identifying and reporting IT security, information security, information management and privacy incidents • Escalating risks, as needed, to their manager
Managers	All managers are responsible for: • Leading and facilitating regular information discussions with their teams • Ensuring their teams are familiar with the Ministry's information policies, guidance; use approved tools, and comply with the Ministry's information governance approach • Providing direction on acceptable behaviours to their teams • Modelling good information practice through their actions and behaviour • Identifying and escalating information risks, as appropriate, to ensure it is managed effectively at the appropriate level and in a timely way • Reporting any IT security, information security or privacy incidents to their line manager
Information Asset Owners	All information assets owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored. The information asset owner must be someone who understands the value of the asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information. At MSD, Information Asset Owners will typically be DCE, Regional Commissioners or Group General Managers.
Information Stewards	Information Stewards are responsible for the quality, integrity, and responsible use of information assets, enabling the organisation to gain maximum value from the information. They are also responsible for supporting information asset owners to make informed decisions about the management and use of their asset for the duration of its lifecycle. The Information Steward must keep the Information Asset Owner informed and made aware of any risks or concerns surrounding the integrity or safety of information. At MSD, Information Stewards will typically be General Managers, Regional Directors and Directors.
Information Governance Committees	Information governance committees are responsible for overseeing and tracking the achievement of the Ministry's strategic objectives relating to information governance.

RELEASED UNDER THE OFFICIAL INFORMATION ACT
Approved by Organisational Committee 2022

Person/Party	Responsibility
	They set the overall risk culture for the Ministry which guides the way it responds to information risk and opportunity. These governance bodies must have membership from the Ministry's Leadership Team, as well as appropriate Māori representation, and have oversight of: • Information and IT security policies and strategies • Information standards and architecture • Obligations contained in the Protective Security Requirements (PSR), the Privacy Maturity Assessment Framework (PMAF), and the Archives New Zealand Information and Records Management Standard • Ministry decisions about ensuring there are adequate systems, processes, and controls in place to identify and manage information risk. At MSD, the Information Governance Committees consist of the Leadership team (LT), Organisational Health Committee (OHC) and the Technical Design Committee (TDC).
Executive Sponsor Information	The Executive Sponsor champions the importance of information management among the organisation's leadership. The aim is for everyone in the organisation to see information management as an integral part of a business operating effectively. The Executive Sponsor Information is responsible for: • Ensuring that the strategy and policy adopted by the organisation supports information management • Being involved in strategic and operational planning to align information management with the corporate objectives and business activities of the organisation • Liaising with business units to ensure that information is integrated into work processes, systems, and services • Overseeing the budget for information and ensuring the resources needed to support information are known and sought in funding decisions • Ensuring that staff with appropriate skills to implement information strategies are employed, and regular upskilling is available • Monitoring and reviewing information to ensure that it is implemented, transparent and meets business needs The CE has delegated the Executive Sponsor Information role to the DCE Organisational Assurance and Communication (OAC).
Chief Security Officer	The Chief Security Officer (CSO) is responsible for having oversight of the Ministry's protective security practices in line with Protective Security Requirements (PSR). At MSD, the CSO is the DCE Organisational Assurance and Communication.
Chief Information Security Officer	The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency. The CISO is responsible for cyber security requirements, and accountable for representing cyber security, leading a programme of cyber security continuous improvement, and managing a virtual team through a distributed security function. At MSD, the CISO is the General Manager (GM) Information. The GM Information is responsible for implementing and having assurance over this policy.

RELEASED UNDER THE OFFICIAL INFORMATION ACT
Approved by Organisational Assurance Committee 2022

Person/Party	Responsibility
Chief Privacy Officer	The Chief Privacy Officer (CPO) sets the strategic direction for Privacy within their agency. The CPO is responsible for: • Dealing with any complaints from the Ministry staff or clients about possible privacy breaches • Dealing with requests for access to personal information, or correction of personal information • Acts as the liaison for the Ministry with the Office of the Privacy Commissioner • Advising the Ministry on the potential privacy impacts of changes to the organisation's business practices • Overseeing the function governing what the Ministry can and cannot do with personal information. At MSD, the CPO is the GM Information.
Chief Analytics Officer	The Chief Analytics Officer (CAO) oversees the analytics function, including data analytics and data science. They set strategic priorities for this function and identify new opportunities for the Ministry based on data. The CAO is responsible for: • Managing the analytics needs across the organisation • The creation of data warehouses • Data governance and data management frameworks At MSD, the CAO is the GGM Insights.
Information Group	Information Group is responsible for: • Supporting MSD's strategic future – providing thought leadership on information security, privacy and information management across, as well as influencing information maturity growth across MSD and all of government • Delivering assurance - providing support to MSD in meeting its compliance responsibilities through an assurance programme to manage defined information risks • Providing expert advice - providing specialist skills to ensure business processes and systems design align to good practice and comply with information legislation and related regulations • Delivering a foundational capability - providing direction, guidance tools, training and support to ensure information capability improvements can be achieved
Insights	The Insights Group is responsible for: • Supporting the Ministry to use and manage Ministry data, analytics, and evidence • Client and Business Intelligence and data science • Research and Evaluation to analyse data and produce insights that inform decision-making and provide evidence on what interventions work for whom • Data Management and data reporting.

RELEASED UNDER THE OFFICIAL INFORMATION ACT
Approved by Organisational Committee October 2022

Definitions

Word/ phrase	Definition
Information	Recorded information (including data) in any form created or received and maintained as evidence of Ministry business. It includes, but is not limited to, documents, email

	correspondence, datasets, audit logs, text messages, voice recording, social media, and web pages.
Information Asset	An Information Asset is an identifiable collection of information and data recognised as having value to the agency. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Lifecycle	The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion
Information Governance	Information governance is the capabilities, processes, controls, oversight, and assurance relating to information security, privacy, sharing and management. Information governance requires the specification of decision rights and an accountability framework to ensure appropriate behaviour across the information lifecycle. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals.
Information Use	Information Use means everything that is done with information. This means not just active use, but also all parts of the information lifecycle (including collection and disposal). For the avoidance of doubt, information is being used when it is held in a database, even when that database is not actively being accessed.
Information Management	The process by which MSD ensures that information is managed across its lifecycle, such that it is accurate, relevant, and accessible; and that it is retained and disposed of appropriately in line with its value and its risk profile.
Information Security	Information Security relates to the protection of information regardless of its form (electronic or physical). The accepted definition of information security within government is: "measures relating to the confidentiality, availability and integrity of information".
Privacy	Privacy relates to the rights you have to control your personal information and how it's used. There is an obvious overlap between information security and privacy. This policy recognises the interdependence of one to the other.
Risk culture	The level of risk that an organisation is prepared to accept in pursuit of its objectives.

RELEASED UNDER THE OFFICIAL INFORMATION ACT
Approved by Organisation

Recording Standard

Approved by:	Privacy & Security Oversight Board (PSOB) on 13 April 2022
Next Review Date:	April 2024
Owner:	General Manager Information

1 Overview

1.1 Purpose

1.1.1 This standard sets out the minimum requirements to ensure that MSD meets its obligations under the Privacy Act 2020 (Privacy Act) when making recordings for operational purposes.

1.2 Definitions

1.2.1 **Recording** refers to speech or moving pictures that have been captured to be listened to or watched later. It does not refer to the process or business of storing them.

1.2.2 **Meeting** is an occasion when people come together, either in person or online, to discuss something, and can include announcements.

1.2.3 **Internal Event or event** means a meeting that is only attended by MSD personnel.

1.2.4 **Client meeting** is any meeting or discussion with an MSD client regardless of whether this interaction is face to face, phone based or via other methods.

1.2.5 **External event** is any meeting, community gathering, function, or a public event that is attended by non-MSD personnel and is hosted or attended by MSD personnel.

1.3 Scope

1.3.1 This standard **must** be applied, using the operational guidance, when recording:

(i) Any images through **CCTV**

(ii) Inbound and outbound calls at the **Contact Centre**

(iii) Any **external events** MSD hosts, attends, or for internal or external public relations purposes.

(iv) An **internal event**

(v) A **client meeting**

1.3.2 This standard **must** be applied by all staff, third parties and contractors who record, or handle recorded information, on behalf of MSD.

1.3.3 This standard **must** be applied equally to formal interviews as well as less formal conversations and other interactions that are recorded.

1.3.4 MSD must grant reasonable requests from non-MSD personnel to record their interactions with MSD.

RELEASED UNDER THE OFFICIAL INFORMATION ACT
APPROVED

2 Standard

2.1 General

2.1.1 There **must** be a clear purpose and justification for recording the meeting.

2.1.2 All parties **must** be able to understand why the recording is happening.

2.1.3 Any reasonable objection or instruction from an attendee **must** be considered, such as a request:

(i) Not to capture their image

(ii) Not to capture their voice

(iii) To note their objection or instruction.

2.1.4 If a reasonable objection or situation is present that prevents recording, a formal record of the events **must** be made via other means i.e., minutes etc.

2.2 Access and retention

2.2.1 Any recording **must** be stored in line with the guidance for managing Ministry information.

2.2.2 Any party to a recording **must** be able to request access to a copy of this, as it is classed as personal information we hold about them.

2.2.3 Any recording **must** only be retained for as long as it is required in line with the original, or a directly related, purpose.

2.3 Use

2.3.1 A recording **must not** be used for a purpose different to, or not directly connected to, the original reason for making the recording.

2.4 Technology and equipment

2.4.1 For recording being facilitated by MSD, only tools approved for recording **must** be used.

2.4.2 If you feel there isn't a tool that meets your needs or would like to check, you **must** contact the Information Management team at infohelp@msd.govt.nz.

2.5 Transparency and notification

2.5.1 The fact a meeting is being recorded, its purpose and the intended use of the recording **must** be understood by all potential and actual attendees and captured as part of the recording.

2.5.2 All those that may be captured in any recording **must** be given reasonable opportunity to consent.

2.5.3 If recording cannot take place without capturing others not party to the meeting or who have not given their consent, then the recording **must not** be created and an alternative method of capturing the information should be used.

2.5.4 If it becomes apparent after a recording has taken place that someone was unexpectedly included in the recording all reasonable steps **must** be taken to resolve the situation in accordance with the process set out in the operational guidance.

RELEASED UNDER THE OFFICIAL INFORMATION ACT
Approved 19 April 2024

2.5.5 Participants **must** be given reasonable opportunity to access or review the accuracy of any minutes or transcription created from a recording, if requested.

3 Standard Compliance

3.1 Exceptions

3.1.1 Any exception to this Standard **must** be approved by the General Manager Information in advance.

3.2 Compliance Measurement

3.2.1 A review **must** be carried out at least once every three years or more frequently (based on the nature and level of risk connected to the process) to ensure that any recording made of handled meets the actions required under this standard.

3.2.2 Compliance to this standard will be measured through the assessment of retention and deletion activities, use of, and fulfilment of any related Privacy Act requests for personal information connected to recordings.

4 References

Privacy Act

Operational Guidance (in development)

Data Protection and Use Policy

Information Hub (containing information policies, standards and guidelines)

RELEASED UNDER THE OFFICIAL INFORMATION ACT
Approved 13 April 2022

MSD Survey Standard

Approved by:	Privacy Security Oversight Board (PSOB)
Approval date:	15 June 2022
Next review:	15 June 2024
Standard Owner:	General Manager Information

Introduction

The Ministry of Social Development ("the Ministry") often surveys clients, staff, stakeholders, and the public to help inform insights into our performance or areas for improvement around projects, programmes and initiatives being undertaken.

Surveys may be undertaken by the Ministry alone, in partnership with another organisation, or by a third party creating and conducting surveys on the Ministry's behalf.

This Standard is intended to provide guidance to Business Units who may undertake or facilitate surveys on the Ministry's behalf, and to set out the basic requirements that must be met.

1 Standard

1.1 Applicability

1.1.1 This Standard **must** be applied by any Business Unit that conducts or facilitates a survey.

1.1.2 Surveys **must** only collect information classified at 'Unclassified' and 'In-Confidence', in accordance with MSD's Information Classification Standard.

1.1.3 The Information Group **must** be consulted immediately if, for any reason, a survey relates to information classified above 'In-Confidence' (i.e., 'Sensitive' or 'Restricted').

1.2 Definitions

1.2.1 "Survey" means research questions on one or more topics, to which people are invited to voluntarily respond to for the purposes of gaining insights.

1.2.2 "Personal information" is any information about a specific individual. The information does not need to name the individual, if they are identifiable in other ways, like through their home address (it does not include a company, or a Trust, or an NGO).

1.2.3 "Collection" includes collection by phone, mail, email, the internet, in person, on social media, or through a specialised survey tool.

1.2.4 "Bias" is an inclination or prejudice for or against one person or group, especially in a way that could be considered to be unfair.

1.2.5 "Discrimination" is an unjust or prejudicial treatment of different categories of people, especially on the grounds of race, age, sex, or disability.

1.2.6 "Responses" to questions may be yes or no, on a scale, multi-choice, or free text.

1.2.7 "Conducting" a survey includes (but is not limited to):

RELEASED UNDER THE OFFICIAL INFORMATION ACT

- creating survey questions
- choosing participants
- distributing the survey
- collecting responses
- storing responses
- analysing responses
- sharing responses or analysis of responses with others (whether inside the Ministry or externally)
- disposing of responses.

2 Meeting the Standard

2.1 Demonstrating compliance

2.1.1 Compliance with this Standard **must** be clearly documented and agreed by the Control Owner or relevant Manager responsible for the Survey.

2.2 Purpose and collection

2.2.1 The Business Unit **must** document a clear purpose for the survey and the rationale for each survey question and associated collection of information from participants.

2.2.2 The Business Unit **must** engage the Information Group to review survey questions **if** any personal information is likely to be collected.

2.2.3 Prior to conducting any survey participants **must** have the purpose for collection and use of information explained to them.

2.3 Transparency and consent

2.3.1 Participation in all surveys **must** be voluntary, and it **must** be clear that participation is voluntary.

2.3.2 There **must** be clear, relevant, and accessible information made available for all participants in advance of their consenting to participate.

2.3.3 At a minimum, the information **must** make clear:

- what the purpose of the survey is
- that participation is voluntary and that a decision not to participate will not affect a prospective participant's relationship with the Ministry
- whether responses will be kept anonymous or whether the participant will be identifiable
- how responses will be used by the Ministry or by others
- who will view the responses (e.g., if they are to be shared with other organisations, which organisations will view the responses)
- what will happen to the survey responses on completion of the survey (e.g., analysis, storage, destruction, etc.)
- [**if** personal information is being collected] that those individuals have the right to access and correct information collected about them; and that they are provided with appropriate MSD contact information.

2.4 Anonymising surveys

RELEASED UNDER THE OFFICIAL INFORMATION ACT

2.4.1 Where identifying an individual is not necessary, there **must** be a process in place to ensure that no personal information is collected. Surveys **must not** include free-text fields for this purpose.

2.4.2 **If** surveys need to include free-text field the Information Group **must** be consulted for guidance.

2.4.3 Where identifying an individual is not necessary, the participants of the survey **must** be advised not to enter any personal information into the survey.

2.4.4 There **must** be a documented process for removing and destroying any unexpected collection of personal or identifiable information that participants supply in response to the survey, as per the Ministry's Information Retention and Disposal Standard.

2.4.5 Where identifying an individual is necessary, but their personal information is not necessary for research and evaluation, there **must** be a process in place to ensure that the information is de-identified.

2.4.6 Where participants need to create a profile or log-in to use a survey tool, usernames and passwords **must** meet the MSD Password Standard.

2.5 Research and Evaluation responsibilities

2.5.1 Surveys with the **explicit** purpose of Research and Evaluation **must** have their survey questions reviewed by the Research and Evaluation team to reduce the risk of unintended bias or discrimination. An Ethics assessment form must be completed and sent to the Information Group.

2.5.2 Consistent with 2.4, if personal information is collected from surveys, it **must** be de-identified after relevant research and evaluation purposes are met.

2.5.3 If analysis of a survey creates or reveals data capable of identifying an individual, the Privacy team **must** immediately be contacted for advice.

2.6 Tool selection

2.6.1 The method or tool used for publishing or submitting the survey **must** be certified and accredited, with its use approved by the Ministry and the Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO). The Information Group can be contacted to confirm a method or tools certification status.

2.6.2 The method or tool used **must** be appropriate for the purpose intended and be used in the way for which it has been approved. Some tools have been approved at MSD Enterprise level. See 3.2 for further details and their accompanying patterns to ensure use is consistent with Information Group expectations.

2.7 Managing bias and discrimination

2.7.1 Care **must** be taken to ensure that the end-to-end conduct of surveys does not introduce bias or discrimination at any point. Bias or discrimination may be introduced through the creation of inappropriate survey questions, the selection of participants, the distribution of surveys, access to surveys, and the analysis and implementation of survey responses.

2.7.2 If surveys have the potential to include or introduce any bias or discrimination, or it is uncertain if they will, the survey **must** be reviewed end to end by the Information Group to minimise any potential risk.

2.7.3 Where surveys produce results that are (or appear to be) biased or discriminatory, steps **must** be taken to identify and remove or mitigate the unintended bias or discrimination.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

2.7.4 Accessibility options for surveys **must** be explored to ensure that those who may not be able to engage with surveys through conventional methods and tools are still able to have their responses collected.

2.8 Engaging with third parties

2.8.1 When using a third-party to deliver a survey or part of a survey, the Third-Party Assurance Standard for Information **must** be met.

2.8.2 If the third-party cannot meet the Third-Party Assurance Standard, the Information Group **must** be consulted immediately.

2.9 Retention and access to data

2.9.1 Access rights of MSD staff members (or third-party) to the information **must** be controlled to ensure that user access is controlled, and access removed when no longer required.

2.9.2 Any survey related information including participants details and responses **must** be managed in a secure manner in accordance with the Ministry Information Retention and Disposal standard, including being stored in an appropriate corporate information repository such as Objective (EDRMS).

3 References

3.1.1 Key artefacts used as inputs in the development of this Standard or that directly support the application of this Standard.

Third-party Assurance Standard

Third-party Assurance Standard – operational guidance

Information Classification Standard

Privacy Policy

Information Retention and Disposal Standard

MSD Password Standard

Research and Evaluation Team - Ethics Toolkit

3.2 Draft patterns to be approved at a later date:

3.2.1 SurveyMonkey – Attestation Document Template (A14199362)

- Recommended to be used for activities, such as Anonymous surveys, non-sensitive information.

3.2.2 Citizen Space – Attestation Document Template (A14303716)

- To be used for activities, such as Engagement and consultation with members of the public, or surveys which may or may not permit anonymous responses.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Personal information use scenarios

Learn about acceptable use of personal information in Microsoft Teams and Workspaces

Please note:

The privacy scenarios below are not exhaustive, and they may not apply directly to your own work at MSD. If you are unsure how to apply any of these acceptable use scenarios, then we advise you to be cautious and not share personal information using MS Teams or Workspaces.

If you want to use personal information in a way that does not align with any of the acceptable use scenarios, then you must consult with Privacy and Information Sharing first using one of the following channels:

- Lodge a request for a Microsoft Teams site/Workspace and indicate that you want to use personal information, and Privacy will be in touch to discuss your request.
- Use of Microsoft Teams/Workspaces will be monitored and as a result some changes may be made, which could include removal of a Microsoft Team if it is unused or misused.
- Microsoft Teams and Workspaces are not information repositories, so you must save the document back to an MSD approved repository and delete the copy in Teams.
- Always remember that any conversations you have in Microsoft Teams, or your Workspace, including in Private or 1:1 Chats, are discoverable - so keep it professional.

Casual / social conversations

We all engage in casual conversations about our personal lives every day. We do it on social media, in emails and in hallways.

You have the choice about if you want to share your personal information in MS Teams Private Chats, Group Chats, or Channel Chats as part of casual non-work-related conversations.

Scenario: You're involved in a casual/social conversation using Teams and everyone is sharing personal details about their lives.

1:1 chat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
It's your choice	It's your choice	It's your choice	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot

Posting your personal information

Just like sharing your personal information during a casual conversation using Teams, you have the right to control how much, if any, information you feel comfortable sharing during virtual team-building activities.

Because team building activities can take numerous forms, and because the choice to participate is in your hands, you can use Teams or Workspaces for sharing your own personal information.

Scenario: Your team is doing virtual team-building activities and you're asked to share personal information, for example contributing to a "get to know your teammates" wiki.

1:1 chat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
It's your choice	It's your choice	It's your choice	It's your choice	It's your choice	No, you cannot	No, you cannot	It's an acceptable use	No, you cannot

Your manager or people leader wants to discuss your performance or have a work-related catch up

RELEASED UNDER THE OFFICIAL INFORMATION ACT

You or your manager are welcome to initiate a conversation about an HR matter or process, or other personal information if you feel comfortable doing so, and provided the conversation is only held within a Private/1:1 Chat.

Scenario: Your manager wants to check in with you to see how your performance development is progressing

1 1 hat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
It's an acceptable use	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot

Only sharing SWN or MSD staff numbers

You can share a SWN or MSD employee number in a Private/1:1 Chat or smaller group chat, only if there is no other identifying or contextual information shared with it (e.g. name, address, client history, employee matter, etc.)

Scenario: You need help determining a client's entitlements so you share the SWN with a senior colleague so they can review the client's details in the CMS

1:1 chat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
It's an acceptable use	It's an acceptable use	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot

You want to share a SWN or employee number and some other contextual personal information about the person

If the information you want to share contains more than one SWN or MSD employee number or there is other personal information included, please see the following scenarios below.

Scenario: You want to discuss or ask for advice about a client or employee with a colleague or manager.

1:1 chat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
It's an acceptable use	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot

Using the private chat / 1:1 function to discuss an issue about a client or employee

You must not have these conversations in a Microsoft Teams channel chat or a group chat that includes a wider group of people/users. Similarly, these discussions cannot be saved into Workspaces in any form.

You must apply very careful judgement about the nature of the personal information you want to discuss in Teams. If it is particularly sensitive, for example gang intelligence information, or an employee bullying matter, it may be more appropriate to use an alternative communication tool (e.g. face-to-face or voice call).

Any decisions and discussions relating to individuals must be captured back into the official line-of-business system.

Keep it professional and remember the Code of Conduct. Always remember that chats are discoverable and can be included in requests for personal information and/or OIA requests.

Scenario: You want to discuss or ask for advice about a client or employee with a colleague or manager.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

1:1 chat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
It's an acceptable use	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot

Sharing a document containing SWNs or employee numbers as a one-off

You may share a document containing SWNs or Employee numbers as a one-off using Private/1:1 Chat, Group Chat, Channel Chat or Workspace Files, if you would usually email the same document.

You must think about who in the Team genuinely needs to see the document. For example, if only 2 other members need to access it then share the document via a Group Chat rather than Channel Chat.

Note: You can also share a link directly to the document from a secure system like Objective or other business repository, if that is more suitable than uploading it to MS Teams.

Scenario: You want to add or upload a document with multiple SWNs or employee numbers as a one-off, i.e. a list of cases.

1:1 chat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
It's an acceptable use	It's an acceptable use	It's an acceptable use	It's an acceptable use	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot

Regularly sharing a document containing multiple SWNs or employee numbers

You may regularly share a document containing multiple SWNs or Employee numbers using Private/1:1 Chat, Group Chat, Channel Chat or Workspace Files, if you would usually email the same document.

Scenario: You regularly share a file with multiple SWNs for staff to work from (e.g. an extracted report from a line of business system)

1:1 chat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
It's an acceptable use	It's an acceptable use	It's an acceptable use	It's an acceptable use	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot

Sharing a link to the report from where you are drafting it instead of uploading the document directly to Microsoft Teams

This means you can manage the access permissions and ensure there are no duplicate copies. You may share the link to the source system using Private/1:1 Chat or Group Chat.

Scenario: You are drafting a report that contains personal information about a client or employee and it is ready for peer review.

1:1 chat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Collaborating on an aggregated or de-identified data set in real time

If you need to collaborate on an aggregated or de-identified data set in real time you can share the data set using Private/1:1 Chat, Group Chat, Channel Chat or Workspace Files, if you would usually email the same document.

Scenario: You want to share a document containing a data set of aggregated or de-identified personal information for research or statistical purposes and you need to collaborate with colleagues in real-time on the analysis.

1:1 chat	Teams group chat	Channel chat	Workspace files	Wikis	Planner	Microsoft Lists	Whiteboard	Forms
It's an acceptable use	It's an acceptable use	It's an acceptable use	It's an acceptable use	No, you cannot	No, you cannot	No, you cannot	No, you cannot	No, you cannot

Need support?

Contact the Information Management Team at infohelp@msd.govt.nz.

Related pages

Workspace Owner Toolkit

How to name your Workspace

Teams meeting etiquette

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Where does information belong?

As employees in the public service we have a responsibility to create and maintain accurate information of our business activities and work so that we meet our obligations under legislation including but not limited to

- Public Records Act 2005
- Privacy Act 2020
- Official Information Act 1982.

We must make sure information is accessible, usable, and managed securely. To achieve this, we need to save it to the appropriate business system. Everyone is responsible for doing this

We create information with varying degrees of value to MSD. To better understand where this information belongs and which environment they should be managed in, refer to the below:

Learn more about no business value | Learn more about short term business value | Learn more about medium-to-high value

RELEASED UNDER THE OFFICIAL INFORMATION ACT

No business value

Not business information as it does not provide valuable context to business transactions, decisions or activities.

Examples:

- copies
- reference documents you've downloaded

Storage options: MS Teams, OneDrive, Outlook.

Short term business value

Is needed for a short-term period to support business transactions, decisions or activities, and does not record or add valuable context in the long term.

Examples:

- meeting notes before they've been written up
- incomplete material used in the preparation of more substantive drafts
- work from home roster
- WAS spreadsheets

Storage Options: MS Teams (for short term storage), OneDrive, Outlook.

Medium to High Value

Is needed for a longer-term period as it provides evidence of our business transactions, decisions or activities

Examples:

- significant versions of a document e.g. a draft being sent for review
- finalised documents
- routine reporting e.g. dashboard reports to Governance Group
- any approvals and authorisations
- something that signifies a policy change or development
- information that provides evidence of consultation
- staff salary details or performance review
- contracts
- Legal case files
- spreadsheets containing de-identified client information

Storage option: Objective/approved Shared Drives, Whaikaha Corporate Information Repository or other approved line of business system.

Note! It's OK to start work on 'medium to high value' information in MS Teams. Once it is ready for a wider audience it must be saved in Objective / Shared Drive (depending on where you work) When it has been moved into Objective, make sure the copy in MS Teams or OneDrive is deleted so there s only one copy of the document. MS Teams is not for long-term storage of information.

How do I?

Learn how to most efficiently do the following activities that are referenced in this guidance:

- Move documents from OneDrive/MS Teams to Objective
- Delete documents from MS Teams
- Delete documents from OneDrive

Please note: All MSD information is managed in accordance with our policies and standards. It is all discoverable under the Official Information Act and covered by the requirements of the Privacy Act and Public Records Act. This includes any of your own personal information that you've chosen to save within MSD systems. If you're not comfortable that MSD will be responsible for the lifecycle (e.g. retention period) of your personal documents, then you're advised not to store them in MSD's storage locations

What if I get it wrong?

To help us prevent sensitive information getting stored in your personal OneDrive, we utilise a Microsoft system called DLP (Data Loss Prevention); which scans all our OneDrive spaces looking for Sensitive Information Types (IRD Numbers, Credit card numbers etc). When a Sensitive Information Type is detected in someone's OneDrive, a member of the Privacy team emails that person to make them aware of the document and provides guidance on how to move it to the correct storage location.

If you receive an email like this, you will need to:

Check the documents you have uploaded, possibly accidently, to your OneDrive Online and remove/delete the ones that contain any MSD Client or Staff personal information (SWN, names, dates or birth, employee numbers, etc) This is especially important if you have finished working on the documents, as we do not want OneDrive to become a repository of personal information.

Please only use personal information in Microsoft Teams and OneDrive Online if it aligns with the Acceptable Use of Personal Information in MS Teams scenarios.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Microsoft Teams Terms of Use

Microsoft Full Teams Terms of Use

- Information of business value must be saved into your existing information repository such as Objective, shared drive or line-of business system. Refer to the Where does information belong guide.
- When using MS Teams Personal Information must only be collaborated on in a private Microsoft Team to ensure it is only available to people with the correct access.
- Information classified as SENSITIVE or RESTRICTED must only be collaborated on in a private Microsoft Team to ensure it is only available to people with the correct access.
- Do not store Ministry information of value in OneDrive. OneDrive is your own storage space and can be used to store personal meeting/working notes or reference material. Ministry information of value must be stored in your existing information repository such as Objective, shared drive or line-of business system.
- Use of Microsoft Teams will be monitored and as a result some changes may be made, which could include removal of a Microsoft Team if it is unused or misused.
- The MSD Code of Conduct, Principles of the Privacy Act and Privacy policy and guidelines apply at all times.
- You must adhere to the Privacy Requirements in the Acceptable Use of Personal Information in M365 guidance.
- Any instances of unauthorised use/access to Personal Information in Teams must be reported to Privacy and Information Sharing Team.

Have some feedback? questions? or suggestions?

Contact us

Microsoft Teams Lite Terms of Use

- Information in Microsoft Teams Lite will be retained for six months, so anything of business value to MSD (e.g. approvals and decisions) needs to be captured elsewhere (e.g. Objective or other line of business systems).
- When discussing information classified as SENSITIVE or RESTRICTED ensure access is limited to only those who need to be involved.
- Use of Microsoft Teams Lite will be monitored, which could result in the removal of Microsoft Teams Lite if it is misused.
- The MSD Code of Conduct, Principles of the Privacy Act, and Privacy policy and guidelines apply at all times.
- You must adhere to the Privacy Requirements in Microsoft Teams Lite Personal Information Use Scenarios.
- Any instances of unauthorised use/access to Personal Information in Microsoft Teams Lite must be reported to Privacy and Information Sharing Team.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Appendix

Ministry of Social Development Information Security Policies – Acceptable Use of Technology Policy

This policy is for all Ministry staff including contractors and consultants.

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

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

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

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

RELEASED UNDER THE OFFICIAL INFORMATION ACT

SharePoint page - Recording Meetings with Microsoft Teams (National Office and Whaikaha)

Terms of Use for Microsoft Teams recording:

You must follow the recording guidance and agree to the below Terms of Use for Microsoft Teams recording prior to being given access. Note: Microsoft Teams recording is not currently available to Service Delivery regional and front-line staff.

- Recordings are permitted with external parties provided all the below terms of use are followed. However, any recordings of client interviews for evidence purposes or discussions relating to any individual MSD entitlements, irrespective of whether the individual concerned is present at the meeting, is strictly prohibited.
- Recording is permitted for meeting organisers only. If you are an invitee or participant you are not permitted to record the meeting.
- Teams recordings are only permitted for approved use cases. If your use case is not listed, please contact the Information Group.
- When organising a meeting, the invite must explicitly state to attendees that the meeting will be recorded. This also needs to be repeated at the start of the meeting prior to turning on the recording functionality. Refer to Booking a meeting.
- You must provide the attendees with the purpose for recording the meeting, what the recording will be used for, who it will be shared with and how they can request a copy of it. Recordings (or transcriptions if the recording has been deleted) must be made available to meeting participants if requested.
- You must give meeting invitees other options for participating if they choose to not attend a meeting that will be recorded.
- Recordings expire after 90 days but should be deleted prior if outlined by the use case. If a recording is required to be retained longer than 90 days, this must be moved to the appropriate site and have the correct retention label applied.

Approved Microsoft Teams Meeting Recording Use Cases:

Purpose of recording	Internal / external meeting*	Use	Storage location
You want to record a meeting to take minutes	Either	Recording should only be accessed by the staff member who is writing up the minutes	The minutes need to be saved into the appropriate repository (e.g. Objective). Once this is complete, the recording must be deleted.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Purpose of recording	Internal / external meeting*	Use	Storage location
You want to record a meeting for staff who cannot attend (instead of rescheduling)	Either	Recording should only be accessed by staff who were in the original meeting invite	Once the staff have viewed the recording from the meeting, it must be deleted.
You want to record content for training purposes	Internal	Recording can be shared internally as education collateral	If the training is required to be retained longer than 90 days, then the recording must be moved to the appropriate Workspace. Otherwise, this should be deleted once no longer required (within 90 days).
You need to record a meeting for someone with accessibility requirements e.g. in meetings where NZSL is to be used	Either	Recording should only be accessed by staff for accessibility needs Where a decision or policy is recorded in NZSL, this can be shared internally.	Where a decision or policy is made in NZSL, then the recording must be moved to the appropriate Workspace. Otherwise, this should be deleted once no longer required (within 90 days).

Note: *External participants are unable to view recordings.

RELEASED UNDER THE OFFICIAL INFORMATION ACT