Justice Centre | 19 Aitken Street
DX SX10088 | Wellington
T 04 918 8800 | F 04 918 8820
ContactUs@justice.govt.nz | www.justice.govt.nz

25 September 2023

Ashley
fyi-request-24009-acd0abb3@requests.fyi.org.nz

Our ref: OIA 107163

Tēnā koe Ashley

Accessing Staff Microsoft Teams

Thank you for your email of 31 August 2023, requesting, under the Official Information Act 1982 (the Act), information regarding the use of Microsoft Teams (MS Teams) at the Ministry of Justice (the Ministry). Specifically, you requested:

> *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. 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?*

In response to your request, I must advise that the Ministry does not hold a specific policy related to managers requesting access to their team members' MS Teams chat log. The use of MS Teams within the Ministry is classified as a means of business communication like emails and telephone calls. Therefore, I am refusing this part of your request under section 18(e) of the Act on the grounds that the information does not exist.

However, please refer to the document schedule appended to this letter which lists the Ministry's policies that can be applied to the use of MS Teams, and my decision on their release. Specifically, we would like to draw attention to the Code of Conduct (page 11), where it states:

> *"The Ministry has the right, without limitation, to monitor the use of Ministry information and technology equipment and systems. This includes the right to access your personal communications and monitor internet use made via Ministry devices and systems."*

All employees, including managers, are required to complete a Code of Conduct learning module every year. A breach of the Code of Conduct, or any other policy, can result in a manager implementing either the Disciplinary Process Policy 2018 or the Unsatisfactory Work Performance Policy 2015.

In response to your second question, I can advise that only two requests to review MS Teams chat logs have been made in the past 12 months. Team members are only notified that a request has been lodged if a disciplinary process has been initiated, in accordance with the Disciplinary Process Policy.

As noted in the Code of Conduct, the Ministry has the right to monitor use of Ministry information and the use of its technology and systems. In practice, requests for access are submitted to the Ministry's People Experience business unit which engages with requestors to understand the rationale for requesting access. Requestors must also complete the ICT request form for secure retrieval of electronic information, which seeks further information about the reason for the request.

Only one request has been approved following this process. We are unable to disclose the justification or reason for that request under section 9(2)(a) of the Act, to protect the privacy of natural persons.

The Ministry expects managers to act in accordance with the Human Resources Delegations Policy, which requires them to make decisions about their people lawfully, reasonably, and fairly. If an employee has reason to believe their manager is acting outside their delegations, or otherwise accessing MS Teams chats or any other information for inappropriate reasons, they may rely on the Ministry's Protected Disclosures Policy. Again, the Code of Conduct Policy (page 5) says:

> *"If you become aware someone is breaching the Code you are required to report this to your people leader, or if necessary, your people leader's manager. Breaches of the Code of Conduct will be addressed in line with the Ministry's disciplinary procedures."*

If you require any further information, please contact Media & Social Media Manager Joe Locke at media@justice.govt.nz.

Please note that this response, with your personal details removed, may be published on the Ministry website at: justice.govt.nz/about/official-information-act-requests/oia-responses/.

If you are not satisfied with this response, you have the right to make a complaint to the Ombudsman under section 28(3) of the Act. The Office of the Ombudsman may be contacted by email to info@ombudsman.parliament.nz or by phone on 0800 802 602.

Nāku noa, nā

Eve Padgett
Acting Deputy Secretary, Corporate and Digital Services

Policies for release

Number	Policy Title	Decision on release
1	Acceptable Use of Technology Policy 2023	Released to you in full
2	Code of Conduct 2023	Refused under section 18(d) as the information is publicly available at: justice.govt.nz/assets/Documents/Forms/Code-of-Conduct-2019.pdf
3	Data and Information Policy 2020	Refused under section 18(d) as it is available at: justice.govt.nz/assets/Documents/Publications/Data-and-Information-Policy-FINAL-2020.pdf
4	Disciplinary Process Policy 2018	Released to you in full
5	Human Resources Delegations Policy 2021	Released to you in full
6	Protected Disclosure Policy 2023	Released to you in full
7	ICT Form – Request for secure retrieval of electronic information	Some information withheld under s9(2)(a) to protect privacy of natural persons

ACCEPTABLE USE OF TECHNOLOGY POLICY

PURPOSE

The purpose of this policy is to establish acceptable use of Information and Communications Technology (ICT) and to explain the duty of care that is expected of us when dealing with Ministry information. We all have an obligation to ensure that our use of ICT does not compromise the reputation of the Ministry or adversely impact our customers or stakeholders.

The Acceptable Use of Technology Policy is designed to ensure that ICT is always used in a manner that is safe, secure and productive for you and our stakeholders.

SCOPE

The scope of this policy includes all aspects of Ministry ICT and data/information including, but not limited to, desktop computers, laptops, mobile computing devices (including Tablets, iPhones and iPads), SMS messages, virtual machines, telephony, printers, scanners, servers, email, intranets, internet access, WiFi, and core business applications.

This policy applies to all users of Ministry ICT including full-time or part-time employees, volunteers, contractors, vendors and personnel affiliated with third parties. This policy applies at all times, during and outside of business hours.

This policy outlines the expectations required of you, but is not a comprehensive list of what you must and must not do. You are expected to apply good judgement when using Ministry ICT systems and handling Ministry records and information. You must consult your manager if you are unsure what this means.

RESPONSIBILITIES

Employee	• Keep informed of the *Ministry's Acceptable Use of Technology Policy* and seek clarification from your manager if required. • Ensure reasonable and appropriate use of ICT in the Ministry by complying with this policy and any other related policies and procedures.
Manager	• Provide advice and guidance to employees regarding the acceptable use of ICT. • Request investigation where reasonable justification has been identified.
Manager ICT Security	• Provide the monitoring, alerting and reporting of any use of technology that might be in breach of the Code of Conduct, and to educate about acceptable ICT use.

General Manager People Experience	• Assist managers to communicate the *Acceptable Use of Technology Policy* to employees. • Work with employees and their managers to investigate and resolve non-compliance issues.

LIABILITY

You are responsible and accountable for the consequences of your actions including any use of Ministry ICT that is inconsistent with the activities of your job purpose or function. If you have any doubt about what the Ministry would consider 'reasonable' you should consult your manager. Any infringement of the Acceptable Use of Technology Policy may result in disciplinary action up to and including dismissal.

OUR POLICY

Quick links

Personal use of Ministry ICT

Protecting Ministry information

Prohibited use of Ministry ICT

Information Security Controls (includes user accounts and passwords, use of external storage devices, installation and modification of software)

Social Media

Using Cloud services

Mobile devices

Relevant legislation

Related policies and procedures

Limit Your Personal Use

Reasonable and appropriate personal use of Ministry ICT is permitted except where that usage impacts network performance, personal productivity or results in undue costs being incurred. You **must** consult your manager if you are uncertain about what constitutes reasonable and appropriate use.

Excessive personal use of the Ministry's technology can impact network performance and productivity, and cause increased costs for the Ministry.

Heavy usage of network data (such as streaming videos, large file downloads) can impact Ministry ICT services for other employees. Heavy usage is monitored and reported on.

You are not permitted to use your Ministry email to register for services that are not business related or approved by your manager.

The Ministry reserves the right to block access to internet sites and services for operational or security reasons.

Notice of monitoring

All email and internet traffic within Ministry networks is monitored, logged and audited. The content of all storage devices, including desktop computers, laptops, file servers, work related mobiles, cloud services and any device connected to Ministry equipment is periodically scanned for malicious, illicit, illegal and inappropriate content.

Monitoring of personal use of Ministry-supplied ICT services and devices is conducted both on an on-going basis and ad-hoc where specially required, in accordance with the Privacy Act 2020. This includes the monitoring of web browsing, emails, instant messaging and applications used to work mobile devices.

Protect Information

You **must** treat all information as a Ministry asset, and protect it appropriately, unless it is clearly identified otherwise.

Inadequately protected information can adversely impact our customers' privacy and the Ministry's reputation.

When accessing or processing Ministry information, you **must**:

- only access information you are authorised to for legitimate work purposes or as required in the course of your duties and consistent with the access provisions of Court Rules, judicial decisions and/or other policies, procedures and guidelines,
- ensure that information is kept appropriately secure by clearing documents from your desk when absent from your work area and from the output trays of printers, faxes and photocopiers,
- lock your screen if you leave your computer unattended,
- report actual and suspected security incidents or weaknesses to either the Service Desk or your manager,
- assess the risks and consequences of unintended disclosure before transferring information outside of the Ministry, especially to non-government parties. This includes transfer by email and portable devices. Consider the use of encryption where the risk and consequences of unintended disclosure are considered unacceptable. Information classified as SENSITIVE and RESTRICTED must be encrypted before transmission.

Unless done so in line with approved business processes, including ICT approval, you **must not**:

- store Ministry information on IT systems outside of those managed by the Ministry or transport information between such systems except when explicitly permitted to do so,
- transmit or distribute any Ministry information via any internet or web-based service,
- transmit or distribute any Ministry information via portable hard drives,
- intentionally access, modify or delete material that you don't have authorisation to access, modify or delete.

As example, you must not, without authorisation:

- use personal email or an unauthorised portable storage device to transfer Ministry information,

- store Ministry related information on a personal computer or device,
- use an unapproved cloud service to transfer or store Ministry information.

Prohibited Use

You **must not** use Ministry ICT for any purpose that might violate or infringe upon the rights of others or which might be considered offensive or defamatory. Such prohibited use includes, but is not limited to:

Unacceptable actions could damage the Ministry's reputation, cause harm or distress to others, or breach the law.

- distributing or storing unauthorised material in support or operation of any business activity other than that of the Ministry,
- conducting any illegal or unethical activity,
- knowingly destroying the integrity of any information,
- downloading, viewing, storing or distributing material that is vulgar, profane, insulting, of a sexual nature, or in any way likely to be offensive to other people,
- distributing spam or electronic harassment of any kind,
- defamation of any individual or organisation,
- distributing, storing, or accessing material in a manner that might infringe copyright, patent, trade secret or any other intellectual property rights of any person or organisation,
- accessing, promoting or taking part in gambling or gaming.

Information Security Controls

Our ICT systems are protected by a number of information security mechanisms, including use of user accounts and passwords. You are always responsible for the use of your accounts, and must take all reasonable measures to keep your passwords and other security credentials confidential.

Breaches of the Ministry's security controls can lead to unauthorised access to or loss of sensitive information.

You **must**:

- maintain the confidentiality of your account and password details for any system that holds Ministry related information (including external login portals), and not share them with any other person,
- use passwords that meet the complexity requirements of the *Ministry of Justice Password Guidelines* document.

You **must not**:

- access Ministry ICT systems using any other person's account,
- connect non-Ministry provided equipment (including portable hard drives, mobile phones and CDs) to the Ministry's system

- connect networks (including access points and ad-hoc WiFi networks) to the Ministry's systems,
- attempt to install software (including plug-ins, patches, fixes, and games) from any source regardless of whether a current licence is held other than via a Service Desk request,
- perform or attempt any actions which are designed to circumvent information security mechanisms.

Social Media Services

Social media services (e.g. Facebook, LinkedIn, YouTube, and Twitter) provide facilities for online collaboration and social networking.

Unnecessary disclosure of work-related information on Social Media can damage the Ministry's reputation.

Whether you are using these services at home or from within Ministry systems, you are reminded of your obligations to keep Ministry information confidential and to act in accordance with any applicable laws, including the Privacy Act 2020. For example, you should not publish information about Ministry business or comment in a manner that may harm the Ministry's reputation on any public website.

It is important you are aware that information disclosed on the Internet is implicitly or explicitly placed into the public domain. Once placed into the public domain, information may be used, in a variety of ways, without your knowledge or authority. For example, the Ministry, if appropriate, might use such information in a work-related investigation.

You should be careful about the nature of your posts to services like Facebook, Twitter or Instagram or any other information disclosed to social media services.

Social Media Policy

This section of the Acceptable Use of Technology Policy should be read in conjunction with the Ministry's Social Media Policy.

Cloud Computing

Cloud computing is any IT service outside the direct control of the Ministry and outside the Ministry's network boundary, where the Ministry's information is stored or processed.

Using cloud services that have not been evaluated and approved may result in disclosure or loss of sensitive information.

Examples of cloud computing services are Dropbox, Office365, iCloud, Google Drive/Docs, Amazon cloud drive, and Box.

Although convenient, cloud computing introduces risk to the Ministry environment. Factors such as ownership of data, availability, accessibility, and security controls in place must be considered when utilising cloud services.

You **must not** use any cloud services to host Ministry data unless it is a Ministry approved cloud service endorsed by the Chief Executive.

	Court information and Judicial information[1] **must not** be stored or processed on offshore cloud services without the prior agreement of the judiciary.
Ministry Provided Mobile Devices	Ministry tablets and iPhones are assigned for checking emails, calendar appointments, reading documents and being reachable while mobile. **Loss or inappropriate use of mobile devices could lead to unauthorised access to sensitive information.** You **must**: • update your device when notified to from ICT communications, • consult with ICT if you are travelling overseas to a high risk country (as defined by the Privacy and Security team) and comply with their recommendations for Ministry equipment you may take, • report to the service desk if your device is lost or stolen, or you think it has been compromised. You **must not**: • download applications that could adversely affect the Ministry's reputation, • leave mobile devices unattended in places from which theft is a reasonable possibility such as vehicles parked in public spaces, or left luggage depositories while travelling, • tamper with or modify the base settings on the device. This includes attempting to alter the device's Outlook synchronisation settings or jailbreaking your device.
Personal Devices	You must not use personal devices to access Ministry systems and information except when explicitly permitted to do so. Information on approved personal mobile device usage can be found on Jet: https://jet.justice.govt.nz/how-do-i/mobile-devices-and-services/. When permitted to access Ministry data from personal devices, you must agree to be bound by any and all conditions of use specified by the Ministry including the Ministry's right to revoke your access and/or wipe Ministry data. It is your responsibility to ensure that any Ministry information held within a Ministry-provided system approved for use on personal devices is not copied or transferred to any other non-approved location. The Ministry does not pay for, or reimburse, any costs incurred when using a personal device. If your manager approves you as eligible for a Ministry supplied plan, then this can be used in a personally supplied device. Please note that a supplied Ministry phone plan should follow all acceptable use guidelines.

EXCEPTIONS TO THIS POLICY

Employee	If you identify a legitimate business need which requires an exemption from this Policy, you **must** discuss and agree this with your manager before taking any action which breaches the Policy.

[1] Defined in Schedule 2 of the Senior Courts Act 2016 and Schedule 1 of the District Courts Act 2016.

	You **must not** take any action which breaches this Policy until a formal exemption is granted.
Manager	If there is a sound business reason for requesting an exemption from this Policy, you **must** engage with ICT Security who will endeavour to identify safe alternative ways to meet the requirements of the business. In the event that an exemption from any aspect of this Policy is required, ICT Security will grant a time-bound exemption to identified staff or business functions.
ICT Security and Security Assurance	ICT Security **must** gain the approval of the Chief Information Security Officer (CISO) before granting a formal exemption from this Policy. Exemptions **must** be time-bound and limited to identified staff or business functions. A register of exemptions **must** be maintained. Exemptions **must** be reviewed and modified, re-validated or withdrawn as they fall due.

RELEVANT LEGISLATION

Employees must not use Ministry-provided ICT to distribute, publish, reproduce or transmit any information in a manner that may breach the obligations of the Ministry or its employees under the following or any other relevant New Zealand legislation:

- Privacy Act 2020
- Official Information Act 1982
- Copyright Act 1994
- Public Records Act 2005
- Crimes Act 1961
- Electronic Transactions Act 2002
- Harmful Digital Communications Act 2015

RELATED POLICIES AND PROCEDURES

- Ministry of Justice Information Security Framework https://jet.justice.govt.nz/our-work/strategy-and-direction/information-security-framework/
- Ministry of Justice password guidelines https://jet.justice.govt.nz/how-do-i/create-strong-passwords/
- Security and Usage Guidelines for CMS Users https://jet.justice.govt.nz/assets/ICT/How-do-I/0ca396b112/cms_security_and_usage_guidelines_May_20181.pdf
- Code of Conduct https://jet.justice.govt.nz/our-work/people/code-of-conduct/

- Ministry of Justice Data and Information Policy
  https://jet.justice.govt.nz/how-do-i/guidelines-for-the-data-and-information-policy/
- Privacy & Information Policy and associated Guidelines
  Privacy | JET — Ministry of Justice Intranet

OWNER	GM Resilience and Assurance Services & Chief Information Security Officer	CONTACT	sean.malthouse@justice.govt.nz
LAST REVIEWED	February 2023 (interim version)	NEXT REVIEW	December 2023
APPROVED	Deputy Chief Executive		

MINISTRY OF JUSTICE
Tāhū o te Ture

DISCIPLINARY PROCESS POLICY

PURPOSE

The purpose of this policy is to set out a formal disciplinary process when misconduct or serious misconduct is alleged against a Ministry employee.

POLICY STATEMENT

The Ministry is committed to following a disciplinary process that is fair and reasonable.

The Ministry will follow a disciplinary process that ensures:

- employees are fairly advised of allegations that may lead to disciplinary action being taken against them and of the potential consequences of those allegations
- a fair investigation takes place into allegations made against employees
- employees receive a fair opportunity to respond to allegations made against them
- employees' responses, submissions and other input is fairly considered before a final decision is made
- employees receive a fair opportunity to provide comment as to what disciplinary action should be taken, if allegations against them are found to be established.

SCOPE

This policy applies to all Ministry employees.

OUR POLICY

Definitions

Misconduct: behaviour by an employee that breaches the Ministry's Code of Conduct, a Ministry policy or some other obligation that applies to an employee in their employment, including for example the express or implied terms of an employee's employment, the State Services Commissioner's Standards of Integrity and Conduct, or statutory obligations that may apply to a position.

Serious misconduct: misconduct that by reason of the nature, extent, seriousness or consequences of the employee's behaviour, may destroy or irreparably harm the trust and confidence the Ministry is able to have in the employee.

Investigator: the person who undertakes an investigation into allegations against an employee. The Investigator may be the employee's manager or some other person (internal or external to the Ministry) who is able to investigate allegations properly and impartially. The Investigator may be appointed by the employee's manager or by a Ministry manager senior to the employee's manager. Investigators should be appointed in consultation with HR Business Partners.

Decision Maker: the person who makes a final decision about whether allegations against an employee are established and if so, whether disciplinary action against an employee should be taken. The Decision Maker must be a manager within the Ministry who holds delegated authority to take any disciplinary action that may be a possible outcome of the investigation.

Allegations	Where it is alleged that an employee has engaged in misconduct or serious misconduct the Ministry will write to the employee and: (a) set out the nature of the allegations (b) advise that the allegations will be investigated (c) advise who the Investigator and Decision Maker will be (if known) (d) advise as to the seriousness of the allegations, for example whether alleged conduct may potentially be found to be misconduct or serious misconduct (e) advise as to the potential disciplinary action that may be taken if the allegations are found to be established (f) notify the employee of their right to seek independent advice from their union or a lawyer (g) notify the employee of their right to bring a union or legal representative, or support person with them to any meeting forming part of the disciplinary process (h) provide initial documentation that may support the allegations.
Preliminary meeting	The Ministry will invite the employee to attend a preliminary meeting. The preliminary meeting may occur by teleconference or through audio-visual technology where the Investigator and the employee are based in different locations. The preliminary meeting is a forum for: (a) the Investigator to outline the matters set out above in the section entitled *"Allegations"* (b) the Investigator to outline the process that will be followed by the Ministry to investigate the allegations (c) the employee to identify any person/s the employee believes should be interviewed or any material that should be considered as part of the investigation (d) the employee to provide any initial response to the allegations that they may want the Investigator to be aware of during the investigation. Any initial response the employee chooses to provide is voluntary and the employee is under no obligation to provide an initial response at the preliminary meeting. If the employee decides to provide an initial response to the allegations at the preliminary meeting and the Investigator is satisfied with the explanation the Investigator can, in consultation with People & Performance, decide to conclude the disciplinary process and take no further action. If the employee decides to provide an initial response to the allegations at the preliminary meeting and admits the conduct alleged, the Investigator may rely on that as proof of misconduct or serious misconduct. In these circumstances the Investigator will not be obliged to make further inquiries or hold a substantive interview with the employee, and may choose to proceed to prepare an investigation report.
Investigation	The Investigator will undertake a fair investigation into the alleged facts giving rise to the allegations against the employee. This will usually include: (a) interviewing witnesses to alleged events or other individuals who may have information relevant to the investigation; and (b) gathering and assessing relevant documents or other evidence that may be relevant to the investigation. Prior to the substantive interview, at the next stage, the Investigator will provide the employee with a copy of all relevant documents or other material arising from the investigation (including notes of interviews conducted). The employee will be provided with a reasonable opportunity to consider such material.

Substantive interview	The Investigator will invite the employee to attend a substantive interview. The substantive interview is a forum for: (a) the employee to provide any response, explanation, comment, submission or other input in relation to the allegations or information arising from the investigation; and (b) the Investigator to put questions to the employee about the allegations or the alleged facts or events on which the allegations are based, or information arising from the investigation. The Investigator will consider the employee's responses and other input in forming views about whether the allegations against the employee are established or not.
Investigation report	The Investigator will prepare an investigation report for the Decision Maker. The investigation report should set out: • the alleged facts or events giving rise to the allegations • the inquiries undertaken by the Investigator • a summary of the relevant information obtained during the investigation • a summary of the responses, explanations, comments or other input provided by the employee • relevant documents or other evidence relied on by the Investigator. The Investigator should set out his or her views as to the relevant facts and state whether or not the Investigator considers the allegations to be established, with reasons. The Investigator will provide to the employee a copy of the investigation report in draft and give the employee a reasonable opportunity to consider the draft report and provide comments or input in writing. After considering any input provided by the employee about the draft investigation report, the Investigator may decide whether or not to amend the report. Whether the Investigator decides to amend the report or not, a copy of any written input (or a summary of any verbal input) received from the employee should be attached to the final investigation report. The Investigator will provide a copy of the final investigation report to the Decision Maker and the employee.
Decision Maker preliminary views	After considering the investigation report, the Decision Maker should write to the employee setting out his or her preliminary views as to whether the allegations against the employee are established and inviting the employee to attend a disciplinary meeting. Where the Decision Maker expresses a preliminary view that one or more of the allegations against the employee are established, the Decision Maker should also set out a preliminary view as to the disciplinary action that the Decision Maker considers may be appropriate to take in the circumstances.
Disciplinary meeting	Where the Decision Maker has formed a preliminary view that one or more allegations against the employee may be established the Decision Maker will invite the employee to attend a disciplinary meeting. Where the Decision Maker and the employee are located in different locationsthe disciplinary meeting may, by agreement between the Decision Maker and the employee, occur through audio-visual technology. At the disciplinary meeting the employee will be given the opportunity to provide any response, explanation, comment, submission or other input in relation to the allegations, the investigation report, and/or the Decision Maker's preliminary views. The Decision Maker will consider the employee's input and should, if practicable, make a

	final decision during the disciplinary meeting as to whether or not the allegations against the employee are established. Where the Decision Maker decides that one or more of the allegations against the employee are established, the employee will be invited to provide submissions or other input about what disciplinary action or penalty should be imposed in the circumstances. At the end of the disciplinary meeting, the Decision Maker may make a decision as to what disciplinary action should be imposed and may convey that decision to the employee verbally at first instance. Alternatively the Decision Maker may at his or her discretion give the employee additional time to make final submissions as to the issue of appropriate disciplinary action following the disciplinary meeting. In such circumstances the Decision Maker will not make a final decision about the disciplinary action to be taken until he or she has received and considered the employee's final written submissions or until the timeframe for the employee to provide such submissions has expired.
Decision on disciplinary action	Following the disciplinary meeting the Decision Maker will confirm or notify the employee of his or her final decision in writing. The Decision Maker may also, at the request of the employee, convey his or her decision verbally by such means as are practical and available in the circumstances.
Suspension	The Ministry recognises that suspending an employee from their employment while a disciplinary process is undertaken is a serious matter. Suspension may be contemplated where the Ministry holds concern that there may be a genuine and unacceptable risk to any part of its business, to the integrity of its investigation, to the safety or wellbeing of any person, or otherwise when the temporary removal of the employee from the workplace is considered necessary to prevent, preclude or minimise the risk of potential harm to any person, property or process. There is no presumption that an employee who is suspended will be dismissed. There is no presumption that an employee who is not suspended will not be dismissed. Prior to making a decision to suspend, the Ministry will advise the employee in writing that suspension is being considered pending the outcome of a disciplinary process, and will give the employee an opportunity to provide comment, submissions or other input about whether suspension is appropriate in the circumstances. A meeting will be convened to enable a manager who has delegated authority to make a decision to suspend (per the HR Delegations Schedule) to hear and consider input from the employee about whether suspension is appropriate and to consider possible alternatives to suspension. Potential suspension situations often involve urgency and meetings to consider suspension must often be convened on short notice. Accordingly, meetings to consider an employee's suspension may occur by teleconference or through audio-visual technology where the manager and the employee are based in different locations. Where an employee's suspension is being contemplated, the Ministry may place the employee on special leave on pay for up to two working days as an interim measure. This is in recognition of the urgent nature of possible suspension situations and serves as an opportunity for both parties to take independent advice and make suitable arrangements for the meeting at which the Ministry will hear and consider input from the employee about whether suspension is appropriate. Where an employee is suspended from his or her employment, suspension will be on pay.
Warnings	Where a disciplinary process leads to allegations against an employee being found to be established but results in disciplinary action falling short of dismissal, the Ministry may elect

to warn the employee.

The following types of warnings may be available options:

Verbal warning

A verbal warning will generally be appropriate for misconduct that is low-level or minor in nature.

Written warning

A written warning is more serious than a verbal warning and will generally be appropriate for first instances of misconduct or for low-level misconduct when the employee has previously been given a verbal warning.

Final written warning

A final written warning is more serious than a written warning and will generally be appropriate in instances of:

- serious misconduct that does not result in dismissal
- misconduct where the employee has previously been given a written warning
- misconduct where further misconduct may lead to the employee's dismissal.

All warnings (including verbal warnings) must be recorded in writing. Warnings should specify the conduct the employee is being warned for and advise the employee of the further disciplinary consequences that may follow if the employee acts in a similar way or otherwise engages in further misconduct or serious misconduct.

Warnings may state that they will remain in force for a specified period of time. On the expiry of any such period the warning will no longer remain in force.

Whether warnings remain in force or are expired will be relevant to consideration of what disciplinary action should be imposed should the employee engage in further misconduct. While warnings that remain in force will generally carry more weight in terms of making a decision about the disciplinary action that should be taken, a pattern of expired warnings may also be a relevant factor.

Any warning, including expired warnings, may be relied on by the Ministry as proof that it has previously been made clear to an employee that misconduct or serious misconduct of a particular type is unacceptable to the Ministry. Expired warnings will not be removed from an employee's personal file.

The Ministry does not require any particular type or number of warnings to have been issued before dismissal may become an appropriate penalty for repeated instances of misconduct or serious misconduct. Such decisions depend on the nature, extent, seriousness or consequences of the employee's misconduct or serious misconduct.

Nothing in this policy detracts from the principle that dismissal, including summary (instant) dismissal may be imposed by the Ministry without prior warning in instances of serious misconduct.

Police involvement	Where allegations are made that involve alleged or potential criminal behaviour by an employee, managers must notify their own manager and seek advice from People & Performance. The Ministry has guidelines in place for making a complaint to the Police and managers must not of their own accord involve Police in matters relating to employees except in legitimate emergencies.
Performance management	The process outlined in this policy is a disciplinary process that applies when allegations of misconduct or serious misconduct are made against an employee of the Ministry. Any disciplinary action that may be taken against an employee for unsatisfactory work performance should be addressed in accordance with the Ministry's Unsatisfactory Work

	Performance Policy and not under this policy.
People & Performance	Managers are encouraged to seek advice from an HR Business Partner in relation to all disciplinary matters and processes. Managers must seek advice from an HR Business Partner in relation to any matter that: • may result in dismissal if the allegations against an employee are found to be established • may have involved possible criminal behaviour by an employee.

RESPONSIBILITIES

Employees	• To keep themselves informed of, and comply with, the Ministry's Code of Conduct, policies and procedures of the Ministry, and any legislative requirements that apply to their work. • To comply with the law at all times.
Managers	• To ensure that employees are aware of the standards of conduct and performance required of them in their employment. • To follow fair and reasonable disciplinary processes when required in accordance with this policy. • To seek advice from People & Performance as required in relation to issues of employee conduct, including in relation to formal disciplinary matters and otherwise as set out in this policy.
People & Performance	• To provide advice and assistance to managers as required.

RELEVANT LEGISLATION

- Employment Relations Act 2000
- State Sector Act 1988
- Privacy Act 1993
- Human Rights Act 1993
- Protected Disclosures Act 2000

RELATED POLICIES AND PROCEDURES

- Code of Conduct
- State Services Commission Standards of Integrity and Conduct 2007
- ICT Acceptable Use policy
- Conflicts of Interest policy
- Harassment policy
- Privacy Act and Personal Information policy
- Personal Gain Through Employment policy
- Fraud and Corruption policy
- Protected Disclosures policy
- HR Delegation policy and HR Delegation Schedule

CONTACT	AskHR	OWNER(S)	General Manager, People and Performance
LAST REVIEWED	April 2018	NEXT REVIEW	April 2020
LAST UPDATED	April 2016		

MINISTRY OF JUSTICE
Tāhū o te Ture

HUMAN RESOURCES DELEGATIONS

PURPOSE

The purpose of this policy is to clarify the principles, conditions and accountability for Human Resources (HR) decisions.

POLICY STATEMENT

The Ministry requires its leaders to exercise decisions relating to its people lawfully, responsibly and fairly. This policy sets the parameters within which leaders can make human resources related decisions at the most appropriate level to ensure the Ministry realises its strategic and operational goals efficiently, effectively and in accordance with relevant legislation.

SCOPE

Schedule 6, Section 2 of the Public Service Act 2020 provides that the Chief Executive may delegate the functions and powers of their position to employees of the Ministry and to individuals working in the Public Service as contractors or as a secondee from elsewhere in the Public Service.

This policy applies to all Ministry employees and to any person to whom the Chief Executive delegates HR functions and powers.

OUR POLICY

Levels of delegated authority

The Ministry has adopted a system whereby HR powers and functions are delegated by the Chief Executive to tiers of managers rather than specific individuals. Any person within scope of this policy who demonstrably hold a position at a specific tier or reporting line are empowered to exercise the level of HR delegations pertaining to that tier.

That is, managers who fit within a specified management tier hold the level of HR delegation designated to that tier; unless advised otherwise in writing. There are five levels of delegation; HRD1 – 5. Managers in tiers 6 and below will exercise HRD5.

The delegation assigned to a position is recorded in OrgPlus, the Ministry's online organisational structure tool.

Decision making parameters

The HR Delegations Schedule sets out conditions that must be followed before specific powers and functions covered in the Schedule may be exercised. For example, some of the delegations require managers to consult with, or obtain agreement from, People Experience (PX).

The reason delegations contain certain conditions is to ensure that delegations are exercised fairly and consistently across the Ministry and appropriate advice is obtained, to assist managers in exercising their delegations and to minimise risk to the Ministry.

The holder of an HR delegation cannot exercise any delegation in relation to themselves or otherwise for their own benefit.

	Delegation holders are only permitted to make decisions relating to their own direct reports and their reporting employees. An exception to this principle exists where it is necessary for managers to exercise a broader delegation to efficiently and effectively administer recruitment processes and assessment centres. Such an exception must be approved by the HRD2 delegation holder of the Group or Groups undertaking the assessment centre. A further exception exists for Strategic People Experience Business Partners (SPX Business Partners) to exercise delegation ministry-wide for administrative and record maintenance purposes. HR delegation holders must also comply with the Ministry's other relevant policies and procedures (for example, financial delegations) when making decisions on HR matters.
Revocations, transfers or acting appointments	From time to time delegations may be revoked either temporarily or permanently by the Chief Executive or otherwise altered or amended by the Chief Executive. A person who is properly appointed to a position to which a HRD1 to HRD5 delegation attaches in accordance with this policy (including on a permanent or acting basis, secondment, or pursuant other valid contractual arrangements) will be authorised to exercise the level of delegated authority that applies to the position. No further instrument of delegation is required.
Monitoring	The Ministry is committed to comprehensive and quality assurance of decisions. The following quality assurance checks may be carried out to ensure delegations are being appropriately exercised: • PX team, PX Advisors, SPX Business Partners and Managers should advise managers regarding matters of delegated authority at the time they seek advice or are asked to process the outcomes of a decision. • Payroll, AskHR and employees that support recruitment processes should monitor approval has been exercised at the correct level when implementing decisions made under HR delegations. • When Managers sign the Legislative Compliance Statement they are confirming they have complied with all of the conditions and requirements presented in the Instrument of HR Delegation and with all related policies and procedures. • Risk and Assurance regularly review the exercise of delegated authorities.

RESPONSIBILITIES

Chief Executive	• Determine and delegate the appropriate level of authority on HR matters to managers. Except where provided in this policy, HR Delegations cannot be sub-delegated by anyone but the Chief Executive.
Strategic Leadership Team	• Role model effective decision making and provide guidance to managers on any issues. The key principle is to provide for effective and efficient decision making on day-to-day people issues at the most appropriate level.
People Experience	• Administer the HR Delegation Policy and Processes. • Assist managers, contractors and secondees to appropriately exercise their delegated authorities.
Delegation Holders	• Ensure the HR powers and functions delegated to them are exercised with due care and integrity and in line with communicated guidance and parameters. They must also ensure the decisions they make do not exceed the authority granted to them.

RELEVANT POLICIES, PROCEDURES AND LEGISLATION

- HR Delegations Schedule
- Ministry of Justice Code of Conduct
- Public Service Act 2020
- Employment Relations Act 2000

CONTACT	AskHR	OWNER(S)	General Manager, People Experience
LAST REVIEWED	June 2021	NEXT REVIEW	June 2023
LAST UPDATED	June 2021	APPROVAL LEVEL	Business Committee

MINISTRY OF JUSTICE
Tāhū o te Ture

PROTECTED DISCLOSURES POLICY

PURPOSE

This Policy outlines the procedure through which disclosures can be made to Te Tāhū o te Ture / The Ministry of Justice (the Ministry) under the Protected Disclosures (Protection of Whistleblowers) Act 2022 ("the Act"), and the Ministry's obligations under the Act when receiving a Protected Disclosure.

SCOPE

This policy applies to Ministry employees, ex-employees, people on secondment to the Ministry, and contractors.

OUR POLICY

Protected Disclosures (Protection of Whistleblowers) Act 2022

The purpose of the Protected Disclosures (Protection of Whistleblowers) Act 2022 is to encourage reporting serious wrongdoing in the workplace by providing protections for individuals without fear of retaliation.

The Act promotes public interest by facilitating the disclosure and investigation of serious wrongdoing in the workplace, and protections for individuals who make disclosures.

The new Act, which came into force from 1 July 2022, is an update of the previous Act and sets down new and improved whistleblowing procedures.

The Ministry is committed to complying with the Protected Disclosures (Protection of Whistleblowers) Act 2022.

Serious wrongdoing definition

For the purposes of this policy 'serious wrongdoing' means any act, omission, or course of conduct in (or by) any organisation that is one or more of the following:

(a) an offence:

(b) a serious risk to:

- (i) public health; or
- (ii) public safety; or
- (iii) the health or safety of any individual; or
- (iv) the environment.

(c) a serious risk to the maintenance of law, including:

- (i) the prevention, investigation, and detection of offences; or
- (ii) the right to a fair trial.

(d) an unlawful, a corrupt, or an irregular use of public funds or public resources:

(e) oppressive, unlawfully discriminatory, or grossly negligent, or that is gross mismanagement, and is done (or is an omission) by:

- (i) an employee (if the organisation is a public-sector organisation):
- (ii) a person performing (or purporting to perform) a function or duty or exercising (or purporting to exercise) a power on behalf of a public-sector organisation or the Government.

Direct disclosures to an appropriate authority at any time	If a discloser is not confident about making the disclosure within the Ministry, they may report serious misconduct to an "appropriate authority" at any time, rather than having to go through their organisation first. An "appropriate authority" includes: (a) The head of any public-sector organisation; (b) Any officer of Parliament; (c) The persons or bodies listed here; (d) A membership body of a particular profession, trade or calling with the power to discipline members. An appropriate authority does not include a Minister or Member of Parliament. However, there are rare circumstances in which a disclosure may be made to a Minister (refer to the 'Disclosures to a Minister of the Crown' section for further details).
Protected disclosures	A protected disclosure will only be made where the individual: (a) believes on reasonable grounds that there is, or has been, serious wrongdoing in or by the Ministry; and (b) discloses information about that in accordance with this policy or the Act; (c) does not disclose the information in bad faith.
Procedure for making a protected disclosure	An individual considering making a protected disclosure can seek advice and support from: (a) The Ministry's Risk and Assurance team (b) An Ombudsman An individual wishing to make a protected disclosure should provide information in accordance with the Ministry process set out in this policy. They may provide their disclosure to: (a) The Ministry's Risk and Assurance team (b) Any General Manager or their equivalent (c) A Deputy Secretary (d) The Chief Executive
Receiving a Protected Disclosure	Within 20 working days of receiving the disclosure, the Ministry should: (a) acknowledge the date the disclosure was received and, if the disclosure was made orally, summarise its understanding of the disclosure; (b) notify Risk and Assurance that a Protected Disclosure has been received and any action taken unless it is not reasonable to do so; (c) assess the risk to the disclosing individual for making a disclosure of serious wrongdoing and take any steps necessary to mitigate this risk; (d) consider whether the disclosure warrants investigation; (e) check with the disclosing individual whether the disclosure has been made elsewhere (and any outcome); (f) deal with the disclosure by: (i) investigating the disclosure; (ii) addressing any serious wrongdoing by acting or recommending action; (iii) referring the disclosure to an appropriate authority; (iv) deciding that no action is required; (g) inform the disclosing individual, with reasons, about what the Ministry has done, or is doing to deal with the disclosure.

If the Ministry is unable to complete these actions within 20 working days, they should begin the process and inform the discloser how long it may take.

Before referring a protected disclosure to an "appropriate authority", the Ministry will consult with the disclosing individual and the appropriate authority to which the disclosure may be referred. If relating to fraud or corruption, Risk and Assurance are required to report this to Audit New Zealand as per the Fraud and Corruption Policy.

The receiver should provide updates to the individual and Risk and Assurance at regular intervals throughout the process.

How people are protected

The Ministry will comply with the spirit and intent of the Act and the requirements of this policy.

An individual who makes a protected disclosure has the following protections:

(a) The Ministry will use its best endeavours to keep confidential information that might identify the discloser. However, the Ministry need not keep a disclosing individual's identity confidential if:

- the individual consents to the release of the identifying information; or
- there are reasonable grounds to believe that the release of the identifying information is essential:
  - (i) for the effective investigation of the disclosure; or
  - (ii) to prevent a serious risk to public health, public safety, the health or safety of any individual, or the environment; or
  - (iii) to comply with the principles of natural justice; or
  - (iv) to an investigation by a law enforcement or regulatory agency for the purpose of law enforcement.

Before releasing identifying information for one of the reasons described in paragraphs (i) or (iii) above, the Ministry will consult with the discloser about the release.

Before releasing identifying information for one of the reasons described in paragraphs (ii) or (iv) above, the Ministry will, if practicable, consult with the discloser about the release.

Anyone may seek information and guidance from an Ombudsman about the duty of confidentiality in the Act.

(b) The Ministry will not retaliate or threaten to retaliate against an individual who is an employee (within the meaning of the Employment Relations Act 2000) who has made, or intends to make, a protected disclosure. This means that the Ministry will not:

- (i) Dismiss the individual for making the disclosure;
- (ii) Refuse or omit to offer or afford to the individual the same terms of employment, conditions of work, fringe benefits, or opportunities for training, promotion, and transfer as are made available to other employees of the same or substantially similar qualifications, experience, or skills employed in the same or substantially similar circumstances;
- (iii) Subject the individual to any detriment or disadvantage (including any detrimental or disadvantageous effect on their employment, job performance, or job satisfaction) in circumstances in which other employees employed by the Ministry in work of that description are not or would not be subjected to such detriment or disadvantage;
- (iv) Retire the individual or require or cause them to retire or resign for making the disclosure.

If the Ministry retaliates or threatens to retaliate against an individual who has made or intends to make a protected disclosure, the individual has a personal grievance against the Ministry under the Employment Relations Act 2000.

(c) The Ministry will not treat or threaten to treat any person ("P") less favourably than it would treat other persons in the same or substantially similar circumstances because:

(i) P, or a relative or associate of P:
1) intends to make or has made a protected disclosure; or
2) has encouraged another person to make a protected disclosure; or
3) has given information in support of, or relating to, a protected disclosure; or

(ii) The Ministry believes or suspects that P (or a relative or associate of P) intends to do, or has done, anything described in paragraph (i) above.

(d) The Ministry will assess any risk of reprisal, repercussion, or adverse impacts to anyone from the first report or disclosure. The Ministry will take steps to address any potential for negative impacts to those involved in the disclosure.

(e) The Ministry will take action to keep the individual safe and work with them to provide appropriate support.

(f) An individual who makes a protected disclosure under this policy or in accordance with the Act is immune from civil, criminal, or disciplinary proceedings because of making the disclosure.

(g) The Ministry will provide practical assistance and advice to a discloser about how to make a disclosure under this policy. Advice can be obtained by either discussing this with your manager, or by contacting Risk and Assurance.

(h) The Ministry will monitor the experience of individuals raising concerns throughout and after the process.

An individual who makes a disclosure knowing it is false, or who otherwise acts in bad faith will not be protected under this policy or the Act.

An individual is not protected under this policy or the Act if they disclose legally privileged information or material.

Disclosures to a Minister of the Crown

Where an individual makes a disclosure to the Ministry under this policy or the Act, and they believe on reasonable grounds that the Ministry:

(a) has not acted as it should under the "Receiving a Protected Disclosure" section of this policy or under section 13 of the Act (as the case may be); or

(b) has not dealt with the matter so as to address the serious wrongdoing

the individual is entitled to the protections set out in this policy and the Act for a protected disclosure made to a Minister.

Supporting information

The protections referred to in this policy (as defined in the section "How people are protected" above) apply with all necessary modifications to individuals who disclose information in support of a disclosure made by another person provided the individual who is disclosing the supporting information:

(a) does not act in bad faith; and

(b) discloses the supporting information to the Ministry in accordance with the "Procedure for making a protected disclosure" section of this policy or discloses the supporting information to an appropriate authority.

RESPONSIBILITIES

Manager

A manager that receives a protected disclosure must:

(a) acknowledge in writing disclosures made under this policy within 2 working days;

(b) advise Risk and Assurance;

(c) seek appropriate advice as needed to consider if the disclosure should be investigated;

(d) assess whether a disclosure meets the criteria for being a protected disclosure and whether the disclosure may be true within 20 working days; and

(e) inform the individual in writing whether an investigation will or will not proceed;

Employees

Employees that become aware of a serious wrongdoing defined under this Policy may:

(a) make a protected disclosure as defined in the 'Procedure for making a protected disclosure' section above.

(b) act honestly and in good faith when making a Protected Disclosure.

Risk and Assurance

Risk and Assurance must:

(a) provide guidance and advice to any individual that has made, or is thinking of making a protected disclosure;

(b) provide guidance and advice to managers that have received a protected disclosure;

(c) follow the same procedure as outlined above for managers, if a protected disclosure is made directly to Risk and Assurance; and

(d) record details of protected disclosures made within the Ministry and report as necessary while observing confidentiality requirements outlined in this Policy.

RELEVANT POLICIES, PROCEDURES AND LEGISLATION

Internal policies and procedures:

(a) Protected Disclosures Reporting Form

(b) Code of Conduct

(c) Disciplinary Process policy

(d) Fraud and Corruption policy

(e) Bullying and Harassment policy

Legislation:

(a) Privacy Act 2020

(b) Protected Disclosures (Protection of Whistleblowers) Act 2022

(c) Health and Safety at Work Act 2015

(d) Te Tiriti o Waitangi

(e) Employment Relations Act 2000

(f) Human Rights Act 1993

(g) Harmful Digital Communications Act 2015

CONTACT	Manager Risk and Assurance	OWNER(S)	Manager Risk and Assurance
LAST REVIEWED	April 2023	NEXT REVIEW	April 2025
LAST UPDATED	April 2023	CONSULTATION	Legal, People Experience

MINISTRY OF JUSTICE
Tāhū o te Ture

Secure Retrieval of Electronic Information – In Confidence

Please fax form to s9(2)(a) **Attn: ICT Security Manager**

Note: This form is intended for use as a mechanism for the secure retrieval of electronic information relating to individual staff, for the purposes of review by that individuals team leader or manager and is subject to approval by Human Resources. Please return the original signed document to the ICT Security Manager or their delegate. Signed original are held by ICT Security with completed copies supplied on request.

1. Staff member details

Name of the individual: _____ Location: _____

Period for review from: _____ to: _____

2. Nature of information required *(tick all that apply)*

- ☐ Mailbox review restoration/restore
- ☐ Home Drive restoration/restore
- ☐ PABX call records
- ☒ Internet Audit/Usage Report
- ☐ Other *(please supply details below)*

Please note: Mailbox and Home drive file restoration are only a point in time snapshot. For Mailbox or file restoration out side the current month, only month end back-ups can be utilised and will require multiple restorations for review of information over multiple months. Beyond 12 months yearly tapes are only available. Internet Audit/Usage Report's are open to interpretation and should be treated with caution.

Other: Please provide details

3. Reason for the investigation.

Example: *"A complaint has been received that the staff member has been sending inappropriate Email or Content"*

4. Requested action

Example: *"Please make restored Mailbox available for review by Jo Smith, Court Manager"*

Requester Details:	**Authorising Manager**
Name:	Name :
Title:	Title:
Phone:	Phone:
Date:	Date:
	I herby agree to any resulting costs associated with this request. RC Code:
Signature: _____	**Signature:** _____

HR Delegate Details *(require in most cases)*:	**ICT Completed by**
Name: Paula Matenga	Name:
Title: Senior HR Business Partner	Title:
Phone: s9(2)(a)	Phone:
Date:	Date:
Signature: _____	**Signature:** _____