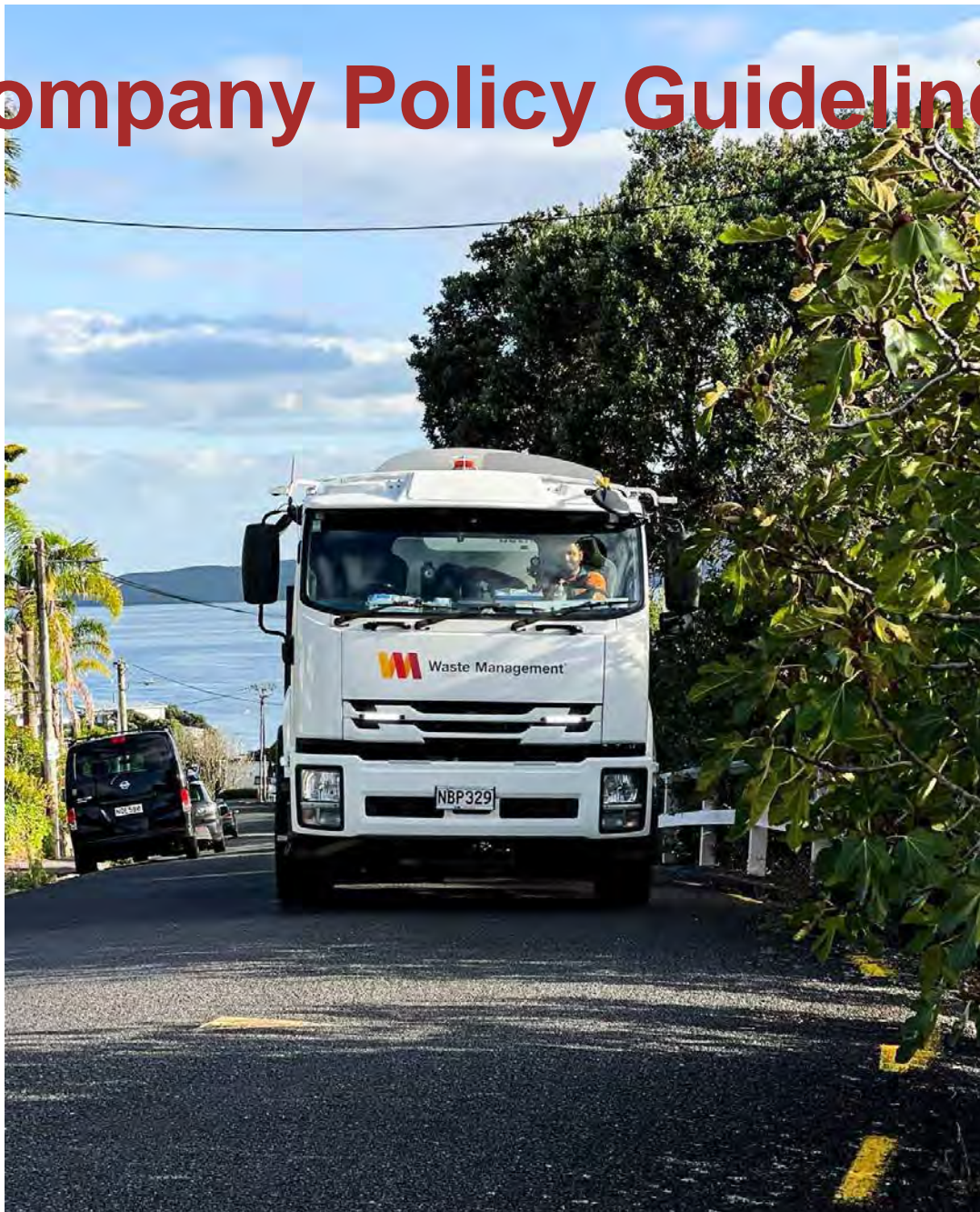




Company Policy Guidelines



Company Policy Guidelines

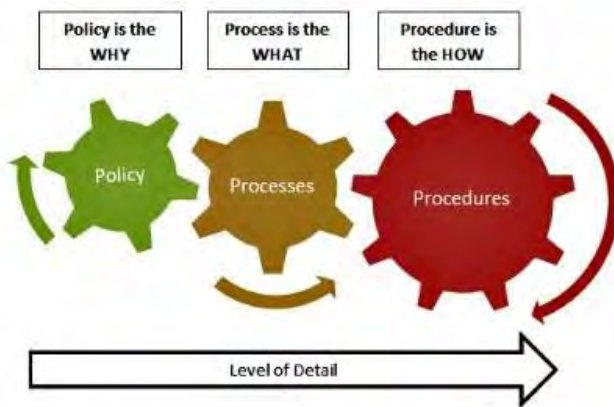
Contents

What is a Policy?	1
Corporate Code of Conduct	2
Health and Safety Policy	5
Drug and Alcohol Policy	8
Epidemic, Pandemic Policy	12
Immunisation Policy	15
Acceptable Workplace Behaviour and Equal Opportunity Policy	19
Speak Up Policy	20
Competition and Consumer Law Policy	23
Safe Driving Policy	32
Acceptable Use of ICT Policy (Under Review)	36
ICT Security Policy	43
Environmental Policy	47
Dress Code Policy	48
Company Policy Guidelines Declaration	51

What is a Policy?

When we talk about policy, one of the first questions that is usually asked is “What is a Policy?”

Policy can mean many different things, but at Waste Management, policies are the business rules and guidelines of the company that ensure consistency and give effect to the company’s strategic direction and ethics. It is a statement of intent used to guide decisions and is implemented through processes.



Policy: The business rules and guidelines of a company that ensure consistency and give effect to the company’s strategic direction and ethics. It is a statement of intent used to guide decisions and is implemented through processes.

Process: A collection of agreed, structured, step-by-step activities which define a clear route to achieving an objective.

Procedure: The specific instructions necessary to perform a task or part of a process. This can take the form of a work instruction, quick reference guide or a standard operating procedure.

Although Waste Management has a range of policies, this booklet contains the essential policies that are the most important to our business. As an employee, you are required to understand and follow these policies, and they will help you figure out what you must do when undertaking certain actions, such as operating a company vehicle or booking business travel. This booklet also contains our commitments and visions that guide our conduct.

We encourage you to become familiar with our policies, which you can read under the policies page of our intranet, along with information about how policies are made, and how they relate to processes and procedures. If you have any questions regarding a policy, please talk to your manager or the Policy Writer directly.

Corporate Code of Conduct

1.0 Introduction

- a) Waste Management NZ Limited ("WM") and its subsidiaries recognises that its reputation is an essential element to its success, and that there is a direct correlation between its reputation and the integrity of the conduct of all those who represent WM.
- b) This Corporate Code of Conduct ("Code") is designed to demonstrate WM's commitment to high ethical standards and behaviour in order to maintain confidence in the integrity of WM. With the support of the Board, this code is binding on all directors, employees, contractors and consultants (collectively defined as "WM Employees").
- c) The content of this code is not intended to cover all possible situations. Rather, it is a reference guide that sets out certain basic principles that should be followed in all dealings related to WM to ensure that WM's business is conducted in accordance with the laws and regulations of all areas in which it operates. Where circumstances arise that are not covered by this code, WM Employees are encouraged to consult their manager or local [People Services representative](#) on an appropriate course of action.

2.0 Promote a Safe and Positive Workplace

- a) WM is committed to providing a safe, healthy and harmonious working environment. All WM Employees are responsible for ensuring that all WM operations are conducted safely, and that the workplace is free from all forms of discrimination and harassment.
- b) WM has implemented appropriate health and safety policies, practices and procedures with the objective of zero harm to our employees and others. All WM Employees are required to follow rules for safe and healthy operations and immediately report any incident which generates an actual or potential injury. They should advise their manager or other relevant management representatives immediately if they see a work practice or activity which they consider to be conducted in an unsafe or careless manner.
- c) WM values the diverse backgrounds of its people and seeks to create an atmosphere of trust, honesty and respect. WM Employees are expected to treat fellow Employees with respect and dignity regardless of gender, race, ethnic origin, religion, marital status or other status. Harassment or discrimination of any kind is not acceptable.

3.0 Enhance the Communities in which we operate

WM takes pride in supporting the communities in which it operates and is committed to building strong community relationships that reflect its values. Additionally, WM is dedicated to providing environmentally beneficial services, products and solutions, and to continually improving our environmental standards. To this end, WM Employees are responsible for understanding relevant [environmental and operating policies](#) and guidelines to ensure that all business activities are carried out with proper regard to the community and the environment.

WM endeavors to ensure all Employees are made aware of relevant legislative and regulatory changes and obligations. WM Employees must take necessary steps to ensure that they fully aware of, understand, and act within in the confines of all relevant laws and regulations covering their individual business areas. If uncertainty regarding the application and interpretation of the law exists, assistance can be sought through the [Legal Department](#).

4.0 Avoid Conflicts of Interest

- a) WM Employee are expected to make decisions that are in the best interests of WM and not for personal gain. WM Employees should not engage in activities or hold or trade assets that involve, or could appear to involve, a conflict between their personal interests and the interests of WM. Such circumstances could compromise or appear to compromise the ability of WM Employees to make impartial business decisions.
- b) WM Employees must not accept gifts or favours of any significant value or give same to anyone

(including clients or suppliers) even though they may believe it will have no bearing on their actions on behalf of WM. In no circumstances may kickbacks, bribes or other illegal consideration be offered, paid, granted, received or accepted by any WM Employees.

- c) If in any doubt about a conflict of interest, the matter should be discussed with [your EMT manager](#) to ensure it is adequately considered.

5.0 Ensure Integrity of Financial and Other Information

Shareholders, management and other interested parties must have complete and accurate financial information in order to make informed decisions.

Many WM Employees participate in the accounting processes that directly impact on the integrity of external financial statements. WM Employees have a responsibility to act in accordance with relevant accounting policies and disclosure requirements and ensure that financial records are recorded in an accurate and timely fashion. Any known inaccuracies must be immediately reported. Unrecorded or “off the books” transactions must not be undertaken for any purpose or in any circumstances.

6.0 Misrepresentation and False Statements

WM Employees must never make deliberate misrepresentations concerning WM or its business operations.

7.0 Protect Confidential Information

- a) Any confidential information including proprietary, technical and financial information must be protected by WM Employees and should be handled on a strict need to know basis. WM's trade secrets should be appropriately safeguarded.
- b) WM Employees should also respect the privacy of individuals and the privacy laws in relation to the collection, use and handling of other people's personal information.
- c) In the course of their work WM Employees may learn of “inside information” about WM and other companies. Employees must not use non-public information for personal profit or discuss such information with anyone who does not have a legitimate business reason to know such information.

8.0 Protection and Use of Property

WM Employees are responsible for the protection and proper use of all WM property used in carrying out their tasks and responsibilities. WM Employees should take reasonable steps to prevent theft, damage or misuse of WM property. This includes the removal by WM Employees of waste products of our customers (scavenging). WM Employees must ensure such property is used efficiently and for business purposes only.

WM property includes tangible items such as inventory, plant and equipment, petty cash, but also includes corporate information and intellectual property such as copyright and trademarks.

9.0 Abide by Competition Laws

- a) All of the business activities in which WM is engaged are highly competitive. It is WM Policy to compete vigorously but fairly. A major part of this commitment is to abide by applicable competition and consumer laws. In general terms these competition laws prohibit WM from collaborating with its competitors to restrain or reduce competition or business rivalry.
- b) WM Employees must abide by competition laws intended to ensure and maintain competition in all markets in which WM operates, and ensure compliance with WM's Competition and Consumer Law Policies. WM Employees must at all times, act ethically and fairly in their dealings with customers, suppliers and the markets in which WM does business.
- c) If WM Employees are aware of any issues which could give rise to anti-competitive conduct they should consult with their manager or the [Legal Department](#) immediately.

10.0 Seeking Assistance

If you have any questions that are not specifically addressed in this Code or any of the WM policies referred to in this Code, please ask your manager or [People Services representative](#) for guidance on whom to contact.

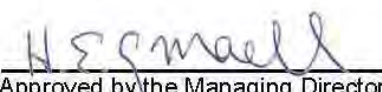
The policies supporting this Code are:

- a) [Health and Safety Policy](#)
- b) [Acceptable Workplace Behaviour and Equal Opportunity Policy](#)
- c) [Environmental Policy](#)
- d) [Conflict of Interest Policy](#)
- e) [Privacy Policy](#)
- f) [Safe Driving Policy](#)
- g) [Competition and Consumer Law Policy](#)
- h) [Speak Up Policy](#)

11.0 Compliance with Policy

Failure to adhere to WM's Code of Conduct may result in disciplinary action which could include termination of employment. If you are aware of any serious misconduct or unethical behaviour that contravenes this Code, any WM policies or the law, you should report this to your manager or make a report under the [WM Speak-up notification service](#). This service is fully independent (managed externally). Full details on how to use this service can be found in the Speak Up Policy.

This code will be reviewed as per the footer date


Approved by the Managing Director

Date: 03/05/2022

Health and Safety Policy

1.0 Objectives

As a Person Conducting a Business or Undertaking, (PCBU), Waste Management NZ Limited and its subsidiaries ("WM"), are committed to the safety, health and wellbeing of our workers. We believe that all workplace related incidents, injuries and illnesses are preventable and aspire to achieve our aim of "Zero Harm" by making health and safety the first priority in all our business activities. We also believe that attaining the highest standards in health and safety is paramount to the success and sustainability of our business.

2.0 Waste Management achieves these objectives by:

- a) Expecting all workers and contractors to cease work if they feel unsafe, or are exposed to health risks;
- b) Consulting with workers and relevant stakeholders in the decision-making processes impacting on workplace health and safety;
- c) Complying with all legal requirements in accordance with [The Health and Safety at Work Act 2015](#), codes of practice and standards applicable to our activities;
- d) Ensuring our systems and processes effectively support the business and our workers to work in a healthy and safe environment;
- e) Demonstrating visible safety leadership through our supervisors, managers, and Directors;
- f) Identifying and understanding the hazards and risks relevant to the activities we undertake and provide effective controls to assess, and manage them accordingly;
- g) Providing appropriate training and support to our workers and contractors to enable them to understand our vision of "Zero Harm", and to allow them to perform their roles competently in line with the health and safety expectations;
- h) Setting objectives, targets and key performance indicators which continually drive us to improve our health and safety performance;
- i) Learning from our performance and continuously improving our processes and work practices; and sharing lessons learnt with others;
- j) Ensuring that all incidents are investigated fully - specifically identifying the causal and contributing factors so that appropriate corrective actions are taken;
- k) Identifying Critical Risks and ensuring these are actively managed;
- l) Regularly undertaking audits and inspections of our operations; and
- m) Communicating this Policy to workers and interested stakeholders; and reporting on our health and safety performance openly and transparently.

3.0 All Officers (Executive Management Team) are required to:

- a) know about workplace health and safety matters and keep up-to-date;
- b) gain an understanding of the operations of the organisation and the hazards and risks generally associated with those operations;
- c) ensure the PCBU has appropriate resources and processes to eliminate or minimise those risks;
- d) ensure the PCBU has appropriate processes for receiving information about incidents, hazards and risks, and for responding to that information;
- e) ensure there are processes for complying with any duty, and that these are implemented;
- f) verify that these resources and processes are in place and being used.

4.0 All Persons in control of a workplace (Regional Manager, Branch Manager, Supervisor) are required to:

- a) Take all practicable steps to ensure the health and safety of all workers while at work;
- b) Ensure that all workers are trained and competent to perform their tasks in line with the company's health and safety processes, procedures, and expectations;
- c) Ensure all HSEQ systems are implemented and followed at all times;
- d) Ensure all workers are able to perform their duties in a health and safe manner (e.g., access to appropriate resources, well maintained plant and equipment, and Personal Protective Equipment ("PPE") relevant to the task; and
- e) Support WM in achieving its objectives set out in [Section 2](#) of this Policy
- f) have a clear understanding of risk and change management and risk identification.
- g) support workers in their understand and application of risk management

5.0 All Workers and Contractors are required to:

- a) Carry out their work in accordance with WM's safety policies, processes and procedures;
- b) Be accountable for their own health and safety, that of others, and ensure their actions or inactions do not create health and safety risks to others;
- c) "SLAM" – Stop, Look, Assess and Manage the hazards and risks inherent to the activities they undertake;
- d) Comply, so far as reasonably able, with any reasonable instruction that is given to them by the PCBU to allow the PCBU to comply with the law;
- e) Stop work if they feel unsafe or exposed to health risks; and
- f) Immediately report any hazards or identified risks and all incidents which cause actual or potential injury, health related issues or damage.

6.0 Worker Health and Wellbeing

- a) Employed workers will be offered and encouraged to have an annual health assessment at WM's cost which may include health monitoring in relation to identified work risks and a general health assessment for the Employee's benefit.
- b) The employed worker will receive all health assessment results. WM will not receive any personal information relating to individual health assessment results, with the exception of health monitoring of work-related hazards.
- c) Non-permanent workers will be assessed, dependant on the task they are completing for WM. Where the task has a potential risk to a worker's health and wellbeing, this will be discussed and reviewed accordingly.

7.0 Children in the Workplace

- a) Due to the nature of our work and risks involved, children under the age of 15 are not allowed to be brought into the workplace under any circumstances. Children over the age of 15 can attend a place of work if enrolled in a recognised work experience programme.
- b) Where workers are required to look after a child / children due to unforeseen circumstances during work hours, carers leave or annual leave are provided as an option, or workers may be allowed to work from home only with approval from a Level 3 manager.
- c) If a worker is on parental leave and would like to attend a workplace to introduce their child to fellow

workers, this must be approved by their reporting manager first. The parent or child must not enter operational areas due to risk.

- d) Open days or pre-arranged site visits that may involve children attending, must be approved by the relevant divisional General Manager who will nominate a worker/s to be responsible for the safe management of the open day or site visit and ensure safety requirements are met.

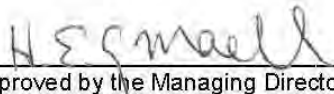
8.0 Application

This Policy applies to all workers, contractors and joint venture partners engaged in activities under WM's operational control.

9.0 Breaches of policy

Any breach of this Policy, including breaches of local procedures, may result in disciplinary action, with potential of formal outcomes up to and including instant dismissal.

This Policy will be reviewed annually.



Approved by the Managing Director
Date: 14 November 2022

Drug and Alcohol Policy

1.0 Objective

Waste Management NZ Ltd and its subsidiaries ("WM") recognise that the highest standards in health and safety are crucial to the success and sustainability of our business and is committed to the safety of all employees, contractors and customers through a zero tolerance policy to alcohol and drugs in the workplace. The Policy applies to employees and, contractors, subcontractor's agency workers and owner drivers("Workers") conducting work for WM on WM sites or customer's sites are bound by this Policy.

2.0 WM achieves the objective by -

- a) Having a zero tolerance to drugs and alcohol in the workplace.
- b) Communicating with employees and contractors on their workplace health and safety obligations in relation to drugs and alcohol.
- c) Providing adequate resources to ensure the successful implementation of this Policy including access to an [Employee Assistance Program](#).
- d) Providing relevant [rehabilitation](#) and awareness to WM employees, to assist in fulfilling their roles and responsibilities under this Policy.
- e) Providing persons attending a WM workplace, or working under its operational control, awareness of and access to this Policy.
- f) Ensuring confidentiality is maintained at all times in respect of these matters.
- g) Undertaking pre-employment, random, post-incident and reasonable suspicion testing for drugs and alcohol.

3.0 Interpretation

For the purposes of this Policy ("work") includes attending workplaces (travelling to and from a place of work), reporting for work and undertaking work activities during working hours. A ("workplace") is a company site at any time and a company vehicle during working hours (this includes travelling to and from work).

If you have access to a WM owned or leased vehicle which can be used for personal use, the conditions of this policy apply at all times when using those WM owned or leased vehicles.

For the purposes of this Policy and the [HSEQ QRG 3.2.1.04 Drug and Alcohol Screening Protocols Quick Reference Guide](#), the "Cut Off" levels for drug use are based on Australia and New Zealand Standards for specimen collection and detection; AS4760-2019 (oral fluids) and AS/NZS4308:2008 (urine).

For all Breath Alcohol testing, WM has set the detection level at 0 (zero) for the workplace. This means any breath alcohol level above 0 (zero) could result in disciplinary action being taken.

4.0 Testing for Drugs and Alcohol in the Workplace

Reasonable cause or post incident testing can be undertaken by either -

- An authorised site representative who has completed an approved training course in using saliva testing kits and breath alcohol testing kits (no authorised site representative can complete urine testing). Refer to HSEQ QRG 3.2.1.04
- WM approved testing contractor (TDDA) or approved medical centre

Random selection testing can only be completed by WM approved testing contractor (TDDA).

Systematic Selection testing can only be completed by WM approved testing contractor (TDDA).

Pre-employment testing must be completed by WM approved testing contractor (TDDA), or an approved medical centre.

5.0 Testing Methods

The following testing methods are approved by WM -

- Pre-employment drug testing is completed by urine sample only.
- Random drug testing is completed using saliva test kits. If a person is unable to provide a saliva sample due a medical condition or other reason, urine testing will be completed.
- Post Incident or Reasonable Cause drug testing is completed using saliva test if the test can be completed within 4 hours of the event. If testing cannot be completed within 4 hours of the event, urine testing will be completed.
- Systematic Selection drug testing will be completed in alignment with the requesting customer or client requirements.
- All breath alcohol testing will be undertaken using an approved breath alcohol testing device.

Note - Inhalants and prescription drugs fall into the "substances" category. These will require a urine or blood test if under pre-employment. If detected during reasonable cause, or post incident, saliva or urine (time dependent) testing will be completed as per HSEQ QRG 3.2.1.04.

6.0 Definitions

The following definitions apply to this Policy, and the [HSEQ ORG 3.2.1.04 Drug and Alcohol Screening Protocols Quick Reference Guide](#), and the Drug and Alcohol screening forms listed in the Protocol -

Drugs means Prohibited Substances and Impairing Substances.

AMP – Amphetamine	MET – Methamphetamine	OPI – Opium
BEN – Benzodiazepines	MOR – Morphine	OXY – Oxycodone
COC – Cocaine	THC – Marijuana	PCP – Phencyclidine

Prohibited Substances means -

- any controlled drug as defined in the [Misuse of Drugs Act 1975](#) ("MODA"), except when possessed or used in accordance with the MODA; or
- any prescription medicine, except when used or possessed under prescription (in accordance with the [Medicines Act 1981](#) and [Medicines Regulations 1984](#)); or any psychoactive substance, other than an approved product as defined in the [Psychoactive Substances Act 2013](#).

Impairing Substances means any substance which may be lawfully sold, possessed, or used, but which has the ability to compromise safety by impairing the judgement, physical coordination, reaction time or concentration levels of those consuming, ingesting or otherwise taking the Impairing Substance, including, without limitation:

- medicines and / or controlled drugs (when not used in accordance with the Medicines Act and / or is a breach of the MODA); or
- approved products as defined in the Psychoactive Substances Act; or
- Alcohol.

Negative Test means a test where the result indicates the level of alcohol and/or drugs in a person's system do not exceed cut-off levels.

Non-negative Test means a test which indicates that the level of alcohol and/or drugs in a person's system has exceeded cut-off levels but where confirmation testing has not yet been completed. After confirmation testing is complete the test result will be reclassified as either negative (not confirmed) or positive (confirmed).

Positive Test means a test which indicates that the level of alcohol and/or drugs in a person's system has exceeded permissible levels where confirmation testing has been completed. In the case of alcohol, confirmation testing would involve a second breath test. In the case of drugs, confirmation testing would involve testing of the split urine sample by an accredited testing laboratory.

DRUG AND ALCOHOL POLICY

Zero Tolerance means the zero-tolerance level for other Prohibited and Impairing Substances will mean a level not exceeding the levels outlined in Drug Tolerance Cut-Off Levels: AS4760:2006 and AS/NZS 4308:2008.

7.0 WM Managers and Supervisors must -

Ensure that confidentiality is maintained of their workers test results and work with their People and Culture Partner when an escalation is required for any issues arising, related to this Policy.

8.0 All workers working for WM and attending our workplaces must -

- a) Ensure they do not work or intend to work under the influence of drugs or alcohol. This must be demonstrated by a negative drug and alcohol test on request.
- b) Never drive or operate any WM owned or leased vehicle, or item of plant (fixed or mobile) while under the influence of drugs (includes certain medications like Tramadol) or alcohol. This includes driving to and from a place of work.
- c) Submit to Drugs and Alcohol testing as requested in accordance with WM's policies, processes, and procedures.
- d) Notify their supervisor or a company representative if they feel unsafe working with one of their work colleagues, because they suspect he / she is in breach of this Policy.
- e) Notify their supervisor or a company representative if they are taking drugs or medication prescribed by a medical practitioner that might impair performance i.e. Tramadol. If appropriate, alternative duties will be assigned on a temporary basis.
- f) If working on a client's site and the worker is under the influence of drugs or alcohol, the worker must comply with the Client's HSEQ Policies and must submit to a Drug and Alcohol test if requested by the Client.

9.0 Compliance with Policy

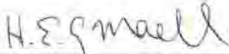
- a) Non-compliance with this Policy may result in performance management action which could include mandatory [rehabilitation](#) processes, reallocation of work duties and responsibilities or termination of employment without notice.
- b) The use of Impairing Substances may be allowable, if WM considers that they are consistent with safe performance of the individual's duties and are being used at the prescribed dosage, if any. The company reserves the right to obtain a professional medical opinion on whether the substance will impair job performance or safety.
- c) Should a worker refuse a lawful and reasonable request to submit to drug / alcohol testing, the refusal to comply may result in disciplinary action. If the manager, after considering reasons given, believe the request is appropriate in the circumstances, please contact your People and Culture Partner for advice or investigation as required
- d) Should a non-employee refuse to submit to drug / alcohol testing while engaged in activities on WM's behalf, and where the request is lawful and reasonable, refuse them access to the WM site. Where safety concerns exist, the site manager should ensure that arrangements are made (preferably with the service provider company) to have the person taken home or elsewhere, where reasonable care can be provided as appropriate in each case; safety being an essential requirement.

10.0 Confidentiality and the [Privacy Act 2020](#)

- a) All information gathered in connection with testing for Prohibited or Impairing Substances, or in participation of rehabilitation or treatment is collected for the purpose of implementing this Policy and ensuring compliance with this Policy.
- b) All information will be held by People Culture and/or the Head of Safety and Risk, and will be held for

- the duration of the individual's employment / engagement or longer, where deemed necessary by WM.
- c) Relevant information may be disclosed to the relevant employee's Supervisor and/or Branch Manager.
 - d) No information relating to any testing or rehabilitation will be disclosed to an external party without the prior written consent of the individual concerned.
 - e) If the employee disputes the test result, they can at their own cost, request a sample for their own analysis.

This Policy will be reviewed annually.


Approved by the Managing Director
Date: 08 August 2023

Epidemic, Pandemic Policy

1.0 Scope

Infectious diseases sometimes develop into epidemics or pandemics and create increased risks for the community. Should the Ministry of Health (MoH) declare a pandemic or epidemic, Waste Management NZ Limited and its subsidiaries (WM) aim to be prepared by having specific policies and controls targeted at the disease and general efforts at preparedness.

2.0 Purpose

WM considers its legal obligations to take all practical steps to protect its customers, Workers (as that term is defined in the Health and Safety at Work Act 2015 (HSWA)), and where possible, the general public from infection or contagion by epidemics and/or pandemics of paramount importance.

- a) WM will facilitate, through its policies and procedures, strategies designed to reduce risks by complying with all directions and/or guidance from authorised public health officers, recognised medical authorities and the MoH, in relation to any pandemic or epidemic.
- b) This Policy applies to all Directors, Executive Management Team (EMT), Officers, Workers, consultants and contractors (including employees of contractors) in the Workplace (as that term is defined in HSWA)) or when visiting customers' sites on behalf of WM.

3.0 Guidelines for WM when preparing for a Pandemic or Epidemic

WM will, as far as reasonably practicable, plan for and make advance preparations for the possibility that its operations will be affected by an epidemic or pandemic, such as COVID-19. This will include but is not necessarily limited to:

- a) Minimising exposure to the disease concerned.
- b) Encouraging and assisting if required, for those who have reason to believe that they are at risk of contracting the relevant disease, to obtain a diagnosis.
- c) Supporting people covered by this Policy (2b) to take reasonable precautions to prevent infection or contagion.
- d) Providing at WM Workplaces, standard precautions such as personal protective equipment where appropriate (e.g. face masks, soap, hand sanitizer, gloves and signage targeting distance, hygiene etc.).
- e) Maintaining the services and operations throughout the period of concern.

4.0 Legislation/Industrial Guidelines and Health Mandates

- a) This Policy is intended to align with any current Government Legislation and key guidance in a response to any pandemic/epidemic.
- b) Where a government vaccination or other health related mandate is issued, and is relevant to work undertaken by WM Workers, or those industries that WM service and support, WM will comply with that mandate on Workers included in the mandate with immediate effect.

5.0 Vaccination

Independently of, or in addition to, any Government vaccination mandates, WM may implement a further policy regarding vaccination if considered necessary to fulfil the purposes of this Policy. Such a policy may make vaccination a requirement of some or all roles within the company and/or precondition for entering WM's Workplaces. Prior to implementing any such policy, WM will:

- a) Undertake a risk assessment process to establish whether the mandating of vaccinations would substantially reduce the risk for Workers of contracting the disease due to the nature of their roles and/or the Workplace.

revisions - please do not remove

- b) Consult with all affected employees and consider all feedback before making a final decision as to the implementation of the policy.

6.0 Guidelines of Wellbeing when in a Pandemic or Epidemic

In the event of an infectious disease being declared a pandemic or epidemic, WM requires all those covered by this [Policy \(2b\)](#) to take the following precautions -

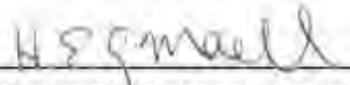
- a) Regularly and thoroughly clean your hands with an alcohol-based hand rub or wash them with soap and water.
- b) Maintain at least 1.5 metres distance between yourself and others, particularly anyone who is coughing or sneezing.
- c) Avoid touching your eyes, nose and mouth, or shaking hands with others.
- d) Make sure you manage good hygiene and encourage others to do the same. This means covering your mouth and nose with your bent elbow or tissue when you cough or sneeze and disposing of used tissues immediately.
- e) Stay home if you feel unwell. If you are well enough to work but would like to minimise the risk of infecting others, ask your immediate manager or supervisor whether you can temporarily work from home.
- f) Keep up to date on the latest hotspots (cities or local areas where the pandemic or epidemic is spreading widely). If possible, avoid traveling to places, especially if you are more at risk.
- g) If you are or are likely to be contagious, notify your immediate manager or supervisor as soon as possible. It may be necessary for you to self-isolate by staying at home until you recover.
- h) Seek medical advice promptly and follow the directions of your local health authority.
- i) Comply with any disease specific advice provided by the MoH.

7.0 Responsibilities

- a) The Managing Director (MD) is responsible for:
 - Nominating the Pandemic Officer. The expectation is the Head of Safety and Risk will be appointed as the Pandemic Officer.
 - Ensuring that any WM Policies are reviewed to be consistent with this Pandemic, Epidemic Policy and all Government instructions.
 - Aligning WM, in the light of the epidemic or pandemic, with the approved Business Continuity Plan.
- b) The Pandemic Officer is responsible for:
 - Working with the MD on the preparation of a comprehensive plan.
 - Leading an Epidemic / Pandemic Risk Leadership Team with an expectation that this will include the of Head of Safety and Risk / Head of People and Culture / Head of Legal and Pandemic Risk Management Team (inclusive of but not limited to – Epidemic/Pandemic Risk Leadership Team and Partners from People and Culture and HSEQ).
 - Advising the MD and EMT on when procedures should be activated.
 - Liaise with relevant Government officials and MOH organisation leaders ensuring the business plays its role in supporting NZ from an epidemic / pandemic waste management position, as well as ensuring the business has up to date information on nationwide Government steps and information to protect WNNZ staff and business.
 - Working with all parts of the business to identify critical Workers and functions.
 - Familiarising staff with recommended procedures regarding disease avoidance.

- Lead management level update meetings to WM management team members L1 – L4's to ensure all leaders are across the approach to be taken to any pandemic or epidemic.
 - Giving notice to Workers, customers, and any persons likely to be affected once pandemic/epidemic procedures are in effect.
 - Ensure business wide communications on the approach to be taken to any pandemic or epidemic are regular and maintained
 - Bringing into operation the pandemic/epidemic management procedure (see Section 3 as a minimum and including any Business Interruption Plan guidelines for a pandemic/epidemic).
 - Instituting any administrative measures necessary to reduce the impact of the vulnerabilities detailed above.
- c) Supervisors and managers are responsible for ensuring that Workers are aware of the pandemic/epidemic procedures in effect at any time.
- d) Workers are responsible for abiding by the pandemic/epidemic procedures specified through communications, when informed by authorised staff those pandemic procedures are in effect.

This Policy will be reviewed annually.


Approved by the Managing Director

Date: 13 October 2022

Immunisation Policy

1.0 Purpose

Both this Immunisation Policy and the [Epidemic Pandemic Policy](#) are in support of Waste Management NZ Limited's ("WM") [Health and Safety Policy](#) – [extract] 2.0 f) *Identifying and understanding the hazards and risks relevant to the activities we undertake and provide effective controls to assess, and manage them accordingly.*

The Immunisation Policy applies to all WM employees, temporary, permanent or contractors who work in roles where they are handling material or in close contact to persons that may expose them to Hep A, Hep B and Tetanus.

2.0 Overview

Many roles within WM (for example working kerbside, on sorting lines, at landfills, in the Technical Services division) could expose workers to diseases that are hazardous to their health and wellbeing.

Impacted roles are included on the following [Appendix 1- Roles Requiring Immunisation](#). This Immunisation Policy provides all workers in these roles with Immunisation from the following diseases –

Hepatitis A

Hepatitis A ("Hep A") is spread through contact with the faeces (poo, tūtae) of an infected person. The virus can cause mild to serious illness in the liver. It can be passed on through poor personal hygiene and contaminated food – including raw shellfish, commercially prepared salads, fruit, and vegetables and frozen berries.

Hepatitis B

Hepatitis B ("Hep B") is passed on through close contact with blood and other body fluids from an infected person. The virus attacks and damages the liver. It was a common disease in New Zealand ("NZ") until a vaccine was introduced in the 1980s.

Tetanus

Tetanus is a serious infectious disease caused by bacteria usually found in the soil. Tetanus is an infection that causes spasms of the muscles. Tetanus bacteria enter the body through wounds such as cuts, grazes and puncture wounds.

3.0 Management Guidance to Immunisation Request

All employees in roles as per Appendix 1, must be immunised and maintain their Immunisation status. An exemption can be made for diseases listed in [Section 2 Overview](#). The Manager has to request an exemption from their [Business Partner - People Culture](#) where it is not practicable for Immunisation to be provided.

The Manager will need to submit a request to the [Employee Onboarding Administrator](#) for their new workers to have a booster against Hep A, Hep B, and Tetanus.

4.0 Existing WM Employees

Employees will provide evidence, if required to fulfill their role, of Hep A, Hep B and Tetanus vaccinations and boosters.

5.0 Covid 19 Vaccination

WM employees are encouraged to keep up to date with Covid 19 vaccination in accordance with current advice from the NZ Ministry of Health.

6.0 References and Further Information

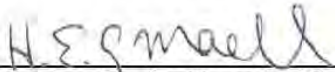
NZ Ministry of Health states on the [NZ Immunisation Schedule](#) that all NZ residents are provided free Diphtheria / Tetanus boosters and Influenza.

New Zealand Ministry of Health – Vaccine Safety: All vaccines approved for use in New Zealand have a [good safety record](#) and have ongoing safety monitoring.

New Zealand Ministry of Health: [Immunisation Handbook 2020](#), (Version 18 released 1 September 2022).
University of Auckland: [Immunisation Advisory Centre](#) website, or you can call 0800 IMMUNE to have your queries answered.

The Immunisation Advisory Centre: www.immune.org.nz

This Policy will be reviewed as per footer.


Approved by the Managing Director

Date 13 October 2022

Appendix 1 – Roles Requiring Immunisation

600 - Business Support	9000 - Operations
612 - Branch Manager	9101 - Auto Electrician
613 - Operations Manager	9108 - Mechanic
614 - Operations Supervisor	9109 - Team Leader – Mechanic
615 - Operations Supervisor - Medical	9119 - Vehicle Maintenance Charge Hand
616 - Technical Services Manager	9120 - Team Leader - Workshop
619 - Branch Manager – TS	9125 - Trades Assistant
622 - Maintenance Supervisor TS	9134 - Maintenance Fitter
624 - Maintenance Manager	9135 - Diesel Mechanic
625 - Operations Supervisor - Fleet	9138 - Electrical Technician
631 - Training and Compliance Coordinator	9412 - Driver - Side Lift / Side Load (4)
634 - Workshop Supervisor	9415 - Team Leader - Driver
635 - Plant Supervisor	9416 - Driver Multi System Operator (2,4,5)
637 - Bin Maintenance and Yard Supervisor	9421 - Driver- Oil Recovery Marine Services
639 - Maintenance Coordinator - Fleet	9424 - Driver General (2,4,5)
641 - Maintenance Supervisor	9428 - Driver (2,4,5)
644 - Operations Supervisor Transport	9429 - Driver – Liquid / Hazardous (2,4,5)
649 - Maintenance & Purchasing Coordinator	9601 - Plant Operator - Earthmoving Equipment
653 - Despatch Coordinator	9603 - Recycling Operator
658 - Operations Coordinator	9610 - Waste Collector Public Spaces Collections
663 - Despatch Supervisor	9620 - Operator - Recycling
665 - Manager - New and Best Practice Tech	9630 - Operator – Organic Waste
675 - Weighbridge and Cust Supervisor	9631 - Operator - Transfer Station
691 - Bin Audit Coordinator	9632 - Team Leader Recycling
	9637 - Operations Supervisor - Production
	9639 - Refinery Operator
	9640 - Kiosk Operator
	9641 - Team Leader – Maintenance Tech
	9646 - Team Leader – Transfer Station
	9658 - Operations Supervisor – Refinery
	9662 - Operator – Hazardous Waste
	9663 - Team Leader - Landfill
	9664 - Operator - Landfill
	9667 - Operator - Liquid and Hazardous
	9668 - Operator - Medical Plant
	9675 - Supervisor - Sort Facility
	9676 - Production Leading Hand LEL
	9679 - Bin Maintainer
	9801 - Bin Puller Runner / Sorter
	9805 - Labourer
	9807 - General Labourer
	9811 - Service Technician
	9814 - Weighbridge and Cust. Assistant
	9825 - Bin Audit Tagger
	9830 - MRF Operator
	9839 - Bin Delivery
	9840 - Greenwaste Monitor (LEL)

800 - Scientific / Technical	Other -
811 - Chemist - Industrials 814 - Laboratory Technician 819 - Environmental Technician 821 - Process Safety Engineer 822 - Electrical Technician - Gas 824 - Generation Manager 825 - Technical Manager 828 - Senior Gas Technician Generation 833 - Technical Manager-Fleet 834 - Gas Technician Generation 835 - Gas Technician Field 836 - Gas Generation Team leader 837 - Landfill Technical 838 - Surveyor 839 - Technical Assistant 840 - Electric Vehicle Technician 841 - Student Engineer 846 - Project Engineer - Fleet 847 - Graduate Project Engineer 848 - Graduate Project Engineer - Fleet 849 - Graduate Project Coordinator 853 - Project Engineer Mechanical Electrical 856 - Project Engineer 857 - Senior Project Engineer 858 - Senior Project Engineer- Fleet 859 - Engineering Technician 861 - Senior Electrical - Mechatronic Engineer - Fleet 862 - Workplace Change Manager 863 - Project Engineer - Elec/Mech 878 - Operations Engineer 879 - Graduate Project Engineer - ME 881 - Technologist 886 - Environmental Engineer	Executive Management Team – Tetanus as a minimum 183 – Regional Manager 237 - Driver Trainer 259 – Compliance Co-Ordinator 260 – HSEQ Partner (300 – Various) Landfill and Recycling administrative staff Sales 412 - Territory Manager - Hunter 413 - Territory Manager – Hybrid 417 - Key Account Manager 421 - Sales Manager 428 - Sales Representative 439 - Sales Supervisor 461 - Sales Manager - National Accounts 464 - National Account Manager 591 - Sales Specialist Landfill 592 - Junior Sales Specialist Landfill 517 - Customer Service Despatch Coordinator

Note: WM Managers, in line with WM Health and Safety Policy, can request other roles (not listed above) to be included for Immunisation.

Acceptable Workplace Behaviour and Equal Opportunity Policy

Waste Management NZ Limited ("WM") is committed to ensuring that it provides a working environment free from all forms of discrimination and harassment. This commitment is based, in part, on the need to ensure that WM complies with the prevailing workplace health and safety and equal employment opportunity legislation.

Furthermore, WM strives to deliver a healthy and harmonious working environment for every one of its employees and to promote professional working relationships based on cooperation and mutual respect between all employees.

WM will use its best endeavours to ensure that in the process of drafting and applying Company policies and procedures that no discrimination takes place and that all employees readily enjoy equal access to opportunities presented within the Company. This Policy of diversification and equal opportunity shall apply to all aspects of employment.

Within WM, each employment opportunity will be determined on the individual merits of the respective applicant. That is, the person selected will be the person who best satisfies the inherent requirements for the position.

WM will not tolerate any form of discriminatory behaviour or harassment, in any of its forms, within the working environment including out of workplace behaviour. Where any form of discrimination or harassment is confirmed, following the appropriate investigations, the persons implicated will be disciplined. In the case of serious discrimination or harassment, or otherwise unlawful discrimination or harassment, being identified, it may result in the termination of the persons responsible.

To facilitate this process, WM has in place the grievance handling and resolution processes (as outlined in your IEA / CEA and in accordance with the [Employment Relations Act 2000](#)) and will ensure that workplace education and awareness programs are delivered and maintained.

Where, as a result of any form of discriminatory behaviour and / or harassment, unsafe working practices or an associated illness or injury are evidenced, it may additionally constitute a breach of WM's Safety Policies.

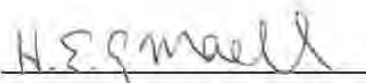
WM confirms that it is committed to delivering the following objectives through its Acceptable Workplace Behaviour and Equal Opportunity Policy:

- a) Ensuring that all employees are treated with respect and dignity and in an equitable manner,
- b) Fully utilising and developing the potential of every employee,
- c) Implement Company policies and procedures in accordance with the Acceptable Workplace Behaviour and Equal Opportunity Policy and principles,
- d) Communicate with all employees to establish an awareness, comprehension and commitment to the Acceptable Workplace Behaviour and Equal Opportunity Policy and its principles.

If you wish to discuss any matter related to this Policy, then please contact the following

- Your supporting manager in the first instance, then
- Regional Business Partner - People and Culture

This Policy will be reviewed as per date on footer


Approved by the Managing Director

Date: 14 November 2022

Speak Up Policy

1. Introduction

The [Protected Disclosures \(Protection of Whistleblowers\) Act 2022](#) ("PDA") is New Zealand's 'whistle-blowing' legislation and replaces the Protected Disclosures Act 2000. The PDA sets out the way employees can report concerns about suspected serious wrongdoing in the workplace. The PDA protects employees who want to and do disclose their concerns in confidence and without fear.

At Waste Management NZ Limited ("WM") we are committed to high standards of conduct and ethical behaviour. The expectation at WM is across all business activities at all levels by all employees. Our policies and [Codes of Conduct](#) have been developed to support this expectation. The Speak Up Policy supports this expectation. It provides a framework for reporting serious misconduct and conduct that is not consistent with the Codes of Conduct and wider WM Policies regarding legal and ethical behaviour.

At WM we want to continuously improve accountability, transparency, and open dialogue on good conduct. That is why WM will investigate all allegations of serious wrongdoing in the workplace including misconduct or unethical behaviour where such complaints are made in good faith. We will protect the identity of the person who reports serious wrongdoing or breaches of this Policy.

The Speak Up service, which is run by a third party service provider is an independent, confidential way for employees to report wrongdoing. Through the use of this service, WM will meet the PDA and protect employees.

2. Purpose

The purpose of the Speak Up Policy is to ensure that employees can report serious concerns anonymously about actual or suspected behaviour that does not comply with the WM Code of Conduct, other company Policies or the law. WM encourages a tolerant 'speak up' culture to help deter wrongdoing and promote accountability.

Where information needs to be given confidentially and/or anonymously, concerns can be reported through the Speak Up 0800 Hotline and/or email address set out below.

Who can use the Speak up Service?

This Policy applies to all employees of WM, at any level of seniority. All WM employees and directors are encouraged to voice their concerns through the [Speak Up Contact Details below](#).

Any person who wants to, can either report the concern to their immediate supervisor, manager, or general manager, or they can go directly to the Speak Up service and report the concern confidentially.

A person who reports any incident or alleged conduct, is referred to as "discloser" in this Policy.

3. What can be Reported?

WM encourages reporting of any concern that the discloser believes on reasonable grounds to contravene internal policies on good conduct and/or serious wrongdoing... Circumstances may include conduct, which is actual, suspected or imminent as follows:

- an offence against any applicable laws.
- a serious risk to public health, public safety, the health or safety of any individual, or the environment.
- a serious risk to the maintenance of the law, including the prevention, investigation and detection of offences and the right to a fair trial;
- an unlawful, corrupt, or irregular use of funds or resources; and
- conduct that is oppressive, unlawfully discriminatory, or grossly negligent, or that is gross mismanagement, by another employee or person in any position.

4. Who can you talk to?

If you become aware of any information that should be reported, you can talk to any of:

- Your immediate supervisor or manager
- A more senior manager
- People and Culture, or
- The independently managed Speak Up 0800 Hotline number below.

5. What Action is taken?

There are two steps to any report, first the report of the conduct and the fact finding step and second an investigation and report. All steps are confidential, and the identity of the discloser remains confidential and is protected.

5.1 Report of Conduct

Once a report is received, a case number is produced. You can refer to this number if you need to provide further information at a later time. A report of the information you have provided is then forwarded to an appropriate person at WMM who is not involved in the alleged incident, conduct, or serious wrongdoing. Your personal details will not be forwarded to the investigator to protect your privacy and identity in accordance with the PDA and this policy.

Where there is an internal report, and internal investigation will be conducted. Where the Speak Up service is used an independent report is prepared for WMM to investigate. WMM will appoint an external independent investigator.

The content of any report relates only to the concern you have raised, and you will not be identified unless you have specifically consented to this. In the first instance, all reports are sent to the Managing Director and the Head of People and Culture.

Alternatively, the following steps may be taken if the conduct relates to the Managing Director, or Head of People and Culture

- In the event that the conduct being investigated is that of the Managing Director, the report is provided to Head of People who shall advise the chairperson of the WMM board.
- In the event that the conduct being investigated is that of the Head of People and Culture the report is provided to the Managing Director who shall advise the chairperson of the WMM board.

If the alleged conduct relates to or is alleged to involve both the Managing Director and Head of People and Culture, then the Head of Legal will investigate and report directly to the chairperson of the WMM board.

If the conduct relates to any member of the WMM executive leadership team, the Managing Director, Head of People and Culture and Head of Legal shall jointly report the conduct to be investigated to the chairperson of the WMM Board.

5.2 Investigation

WMM will then commence a two stage process. The first is to look into the allegations and prepare a report on the facts. This is followed by an investigation to determine whether further action is appropriate. You will be informed of the outcome of the investigation within four (4) weeks through the independent service provider.

Your identity and the fact that you have reported an incident, or any conduct will remain confidential, as will the subject of your report. No details of your participation in this process will be passed to WMM unless you have specifically consented for this to occur.

6. What happens to you when you speak up?

You will be protected for speaking up. The PDA protects you. You are entitled and will receive full confidentiality, and there will be no threats, reprisals, or inappropriate behaviour as a consequence of you reporting an incident or conduct. Any actions of this nature towards you by any person will not be tolerated and would constitute a breach of this Policy and the PDA.

You are also protected by the Human Rights Act 1993. The Human Rights Commission is an independent agency that any person can approach to report any conduct that is an attempt to infringe your human rights, including your right not to be discriminated against for speaking up and to receive fair and equal treatment, with dignity and respect. The details of the Human Rights Commission are set out below.

WM will take all reasonable steps to ensure that adequate and appropriate protection is provided for those who make a report in good faith. This protection applies, regardless of the outcome or whether the matter is referred to an external authority.

7. How do you make contact with the Speak Up Hotline?

The Speak Up 0800 Hotline is operated 24/7. Alternatively, you can use the website below anytime, or download the app and make a report through the app. Current contact details are provided below. Urgent calls made outside these times will be diverted to a mobile phone. In the unlikely event your calls are not answered, a message should be left with your contact details, so an operator can call you back.

The operator taking your call is not employed by WM but provides the service under contract and in accordance with this Policy. No calls received by an operator are recorded (excluding answerphone messages).

8. Speak Up and the Human Rights Commission Contact Details

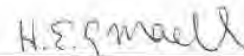
Speak Up 0800 hotline: 0800 753 343

Website: [RAISE - Whistleblower Notification](#)

The Speak Up service is operated by [RAISE](#) who also provide WM's free and confidential Employee Assistance Programme.

Human Rights Commission/Te Kahui Tika Tangata : <https://tikatangata.org.nz/>

This Policy will be reviewed as per the date on the footer.



Approved by the Managing Director

Date: 08 August 2023

Competition and Consumer Law Policy

The purpose of this document is to ensure all employees and representatives of Waste Management NZ Limited ("WM") fully comply with the Commerce Act 1986 and the Fair Trading Act 1986 ("the Acts").

1.0 Application

The Policy applies to WM and all of its respective officers, employees and representatives.

2.0 The Compliance Programme

In furtherance of its commitment to compliance with the Commerce Act and the Fair Trading Act, WM has adopted a Competition and Consumer Law Compliance Programme. The principal components of that Programme are

- a) The establishment of this Competition and Consumer Law Policy;
- b) Compliance training, on a regular basis, for employees who, as part of their duties, have contact with customers and/or competitors or influence WM prices;
- c) The appointment of [Head of Legal](#) as the person to oversee the Programme and to manage competition and consumer related issues; and
- d) The creation of a [reporting process](#) for receiving and handling possible competition and consumer related issues.

3.0 Competition and Consumer Law Policy

It is the policy of WM to comply in all respects with the Commerce Act and the Fair Trading Act and at all times to act ethically and fairly in its dealings with customers, suppliers and the markets in which it does business.

In furtherance of this Policy, **no officer, employee or representative of WM is permitted to do any of the following things:**

- a) Enter into or give effect to any contract, arrangement or understanding with any competitor that contains a cartel provision ("**Cartel Conduct**"). Cartel Conduct includes:
 - i. Price Fixing;
 - ii. Restricting outputs in the production or supply chain ("**Output Restrictions**");
 - iii. Allocating customers, suppliers or territories ("**Market Sharing**"); and
 - iv. Bid-Rigging (a type of Output Restriction).
- b) In any market where WM has substantial market power, use that power with the purpose of eliminating a competitor, restricting the entry of a new competitor or preventing or deterring any person from engaging in competitive conduct ("**Misuse of Market Power**").
- c) In any market in which WM has a substantial market share, discount the price of any of WM's products or services below WM's cost of supplying that product or service for the purpose of eliminating a competitor, preventing the entry of a new competitor or preventing or deterring any person from engaging in competitive conduct ("**Predatory Pricing**").
- d) Enter into any contract, arrangement or understanding that may have the purpose, effect or likely effect of substantially lessening competition ("**Anti-Competitive Arrangement**"). This can include agreeing with a third party the customers or suppliers that WM will do business with or will not do business with ("**Boycotting**").
- e) Except with advice from the Legal Team:
 - i. Supply any good or service to a customer on the condition that the customer not buy from a competitor of WM or limits its purchases from a competitor;

- ii. Provide to any customer a price discount, rebate or credit in return for the customer agreeing not to buy from a competitor or to limit its purchases from a competitor;
 - iii. Refuse to trade with any customer or supplier because it has done business with any other person or company; or
 - iv. Buy any good or service from a supplier on the condition that the supplier not supply any other person or company. ("**Exclusive Dealing**")
- f) Control or attempt to control the resale price to be charged by a customer in respect of goods that the customer purchases from WM ("**Resale Price Maintenance**").
- g) Engage in any conduct when dealing with customers, suppliers or any third party that is misleading or deceptive or that is likely to mislead or deceive ("**Misleading or Deceptive Conduct**").
 - i. Conduct that is liable to mislead the public as to the nature, manufacturing process, characteristics, or suitability for a purpose, of goods or services;
 - ii. Making representations, including in the marketing, advertising or promotion of any of WM's products or services, that have not been substantiated before they are made ("**Unsubstantiated Representations**"); and
 - iii. Making any false or misleading representation in connection with the supply or possible supply of WM's products or services, e.g. by representing that the products or services are of a particular standard or quality when they are not or claiming unpaid debt is owed ("**False or Misleading Representations**").
 - iv. If you have doubts about whether a representation can be substantiated or is false or misleading, please take advice from the Legal Team.
 - v. Fail to comply with the rules when conducting uninvited direct sales (i.e. door-to-door sales) ("**Uninvited Direct Sales**").
 - vi. Include unfair contract terms in standard form agreements ("**Unfair Contract Terms**").

4.0 Responsibilities of Corporate Counsel

Head of Legal as responsible Corporate Counsel has the following responsibilities relating to the Competition and Consumer Law Compliance Programme:

- a) To implement the Compliance Programme and monitor its effectiveness;
- b) To receive and oversee the handling of reports of possible breaches of this Policy or the Acts;
- c) To receive and respond to trade practice questions and issues raised by WM employees;
- d) To report to senior management of WM and the HSERCC Committee of the Board on trade practice issues and the effectiveness of the Competition and Consumer Law Programme; and
- e) To be the point of contact with the Commerce Commission and to receive and oversee WM's responses to any Commerce Commission enquiries or investigations.

5.0 Responsibilities of Company Employees and Representatives

Each employee of WM must:

- a) Obtain advice from the Head of Legal before taking any action if there is any question or concern as to whether that action could breach either of the Acts or this Competition and Consumer Law Policy;
- b) Promptly call the Head of Legal if they receive any complaint regarding a possible breach of the Acts;
- c) Promptly call the Head of Legal if they become aware of any act or occurrence that the employee thinks could be a breach of one of the Acts or could lead to a breach of one of the Acts;

- d) Complete and/or attend Competition and Consumer Law compliance training when offered by WM to each employee who, in the course of the employee's duties has relevant contact with competitors and/or customers;
- e) When requested by management of WM, to confirm in writing that the employee has read and understood the Competition and Consumer Law Policy and agrees to comply with it;
- f) If contacted by the Commerce Commission relating to any investigation or enquiry, to immediately refer them to Head of Legal for comment and then to notify Head of Legal that contact has been made.

6.0 What to do if the Commerce Commission contacts you

- a) It is the policy of WM to cooperate fully with the Commerce Commission in carrying out its responsibilities under the Acts. The Commerce Commission has been advised that all contact with WM should be made via Head of Legal. In no case, should any employee provide information or documents to the Commerce Commission without first advising his or her General Manager and Head of Legal
- b) If the Commerce Commission makes a request for information in writing, that request should immediately be forwarded to Head of Legal to arrange a response.
- c) If the Commerce Commission makes contact by telephone, the employee should state that it is WM's policy to cooperate with the Commerce Commission, politely request that the enquiry be directed to Head of Legal and say nothing further.

7.0 The Commerce Act and Fair-Trading Act

It is not possible to specifically identify every type of conduct that might breach one of these Acts. In some instances, a detailed legal or economic analysis of the market may be necessary to determine whether or not a particular act is illegal.

IF IN ANY DOUBT, WM'S EMPLOYEES MUST CONSULT WITH THE LEGAL TEAM BEFORE ENGAGING IN THE CONDUCT.

Set out below is a brief description of the various prohibitions covered by the Acts and WM's Competition and Consumer Law Policy:

8.0 Cartel Conduct

Any understanding between two or more competitors that amounts to cartel conduct is illegal. An "understanding" can be reached via any sort of communication, or arrangement or in any form of written documentation. It is illegal if it relates to:

- a) Fixing, controlling or maintaining the price at which goods are bought or sold ("**Price Fixing**"); or
- b) Restricting outputs in the production or supply chain, including "Bid-Rigging" ("**Output Restrictions**"); or
- c) Allocating customers, suppliers or territories ("**Market Sharing**").

Even sharing information with a competitor regarding these topics can lead to an inference that there has been an illegal understanding.

Industry meetings and events are high risk, as these are considered a "hot bed" for cartel conduct. There is no industry association defence. In fact, under the Commerce Act, any contract, arrangement or understanding arrived at by an association – or any recommendation made – is deemed to have been entered by all of the association's members. Merely being present, or a passive observer of an inappropriate conversation amongst competitors is sufficient to implicate yourself and WM. In any meeting or situation in which a competitor attempts to discuss any of the above subjects, WM employees must voice their objection and if the inappropriate conversation continues must leave the meeting immediately, having these actions noted in the minutes. The employee should contact the Legal Team immediately following their departure.

Competition law applies equally to social settings as it does to more formal meetings. Comments made in the presence of a competitor at a social function can be used to infer an illegal understanding between the

competitors. Conversations in respect of prices, terms of sale, customers or territories are therefore risky and must be avoided.

8.1 Price Fixing

- a) If an understanding or arrangement is reached between competitors which has the purpose or likely effect of directly or indirectly fixing, controlling or maintaining the price, or any component of price such as a discount, allowance, rebate or credit in relation to goods or services supplied or acquired by WM or a competitor ("**Price Fixing**") then it is illegal.
- b) The law can be breached, not only by arrangements to set a specific price, but also by communications between competitors that have the effect of stabilizing prices, setting a minimum price, fixing the time at which prices will be increased or decreased, or otherwise limiting the independence of competitors in pricing their products or services. Such restraints are illegal even if they affect only a discount, rebate, allowance or a credit applicable to a transaction.
- c) It is the policy of WM that, at all times, the prices for its goods and services will be set independently, without any consultation, understanding or other communication with competitors. Note that, depending on the circumstances, "Competitors" may include Councils and facilities service providers who bid on waste contracts.
- d) In some instances, WM may obtain services from or subcontract to a competitor. It is important to be very cautious in such situations so that any discussion of price or other terms of sale are strictly limited to the immediate transaction between the two companies. Provided such transactions are properly documented and implemented they are likely to benefit from the vertical supply exception.
- e) Examples of conduct that can be used as evidence of price fixing include:
 - i. Supplying price lists to competitors or obtaining price lists from competitors, except in the context of selling to or buying from the competitor.
 - ii. Announcing future prices in advance to competitors.
 - iii. Agreeing with competitors on the date when prices will be increased, even if there is no agreement on the amount of the increase.
 - iv. Agreeing with competitors on terms or conditions that affect prices.

8.2 Output Restrictions

- a) If a provision in a contract, arrangement or understanding between competitors has the purpose of directly or indirectly preventing, restricting or limiting the production of goods, the capacity to supply services, or the supply of goods or services by WM or a competitor ("**Output Restrictions**") then this could constitute cartel conduct and would be illegal.
- b) Output Restrictions agreed between competitors can occur in the form of production or sales quota arrangements or an agreement between competitors to limit the volume of particular goods or services available on the market, irrespective of the effect. It is WM's policy that it will produce goods and supply services and determine its capacity to produce goods and supply services, independently of its competitors.
- c) No employee of WM is permitted, at the request of a competitor, to restrict or limit the production or supply of goods or services to any customer or potential customer. Nor should any employee request any competitor to restrict or limit its production or supply to any customer.

8.3 Bid-Rigging

- a) In the event of a tender process in relation to the supply or acquisition of goods or services any attempt to restrict or interfere with rival bidding in accordance with a contract, arrangement or understanding ("**Bid Rigging**") is illegal. This can include if:
 - i. a provision has the purpose of directly or indirectly ensuring that certain parties bid but others do not, or
 - ii. parties bid on an agreed basis that one of the bids is more likely to be successful, or
 - iii. parties share information relating to their bids;

- iv. certain parties agree to proceed with their bid and others do not, or
 - v. a material component of at least one of the bids is worked out by arrangement between competing bidders
- b) It is WM's policy that it will independently decide which tenders and individual contracts it will bid for and on what terms a bid will be submitted. No employee of WM is permitted, at the request of a competitor, to submit a bid or price quotation to any potential customer that does not represent a genuine attempt to be the successful bidder. Nor should any employee request any competitor to submit such a bid or price quotation. No communication with any competitor on the terms of WM's or a competitor's bid is permitted.

8.4 Market Sharing & Territorial Restraints

- a) If a provision in a contract, arrangement or understanding between competitors has the purpose of directly or indirectly allocating customers or suppliers, or the territories in which goods or services can be supplied or acquired ("**Market Sharing**") then this could constitute cartel conduct and would be illegal.
- b) Market Sharing includes any understanding between competitors to divide or allocate business between them. Territorial Restraints such as agreeing with a competitor on which areas WM will do business, or will not do business, are contrary to WM's Competition and Consumer Law Policy because they are potentially illegal.
- c) Examples of prohibited Market Sharing conduct include:
 - i. Agreeing with a competitor not to produce one another's product, or not to provide the same services;
 - ii. Agreeing with a competitor to use a particular supplier, or not to use a particular supplier;
 - iii. Agreeing with a competitor not to solicit or sell to each other's customers;
 - iv. Agreeing with a competitor not to expand into a market in which a competitor is already established.
- d) It is WM's policy that it will independently decide where and when it will compete for business. No communication with any competitor on this subject is permitted.

8.5 Exceptions to Cartel Conduct

The Commerce Act recognises that there may be legitimate reasons why competitors need to discuss and/or agree on matters such as prices, target markets/customers, or output volumes. While a number of exceptions exist, these are highly technical, so it is important that WM employees contact the Legal Team before relying on them. The main exceptions to cartel conduct are:

- a) **Collaborative activities:** Where the parties are combining their businesses, assets or activities in some way in a commercial activity; the dominant purpose of the collaboration is not to lessen competition between the parties; and the cartel provision is objectively reasonably necessary to achieve that procompetitive or benign purpose;
- b) **Vertical supply contracts:** Where the cartel provision is included in a vertical supply contract and relates to the supply or on-supply of goods or services and the dominant purpose of the provision is not to lessen competition between the parties
- c) **Joint buying:** Where competitors have formed a joint buying group to collectively negotiate and purchase inputs, they may agree to fix the price at which they will collectively acquire these.

However, these exceptions only apply in respect of the cartel prohibition. The agreement must still not have the purpose, effect or likely effect of substantially lessening competition in a market.

9.0 Misuse of Market Power

Conduct that may be permissible for small competitors in a market may be illegal if undertaken by a company that has substantial market power. It is a breach of the Commerce Act for a company to take advantage of its substantial market power for the purpose of:

- a) eliminating a competitor;
- b) restricting the entry of a person into any market; or
- c) deterring or preventing a competitor from engaging in competitive conduct.

Therefore, employees must be particularly cautious in dealing with customers and suppliers in any market where WM has such power. As a general proposition, it should be considered that WM may have substantial market power in any market where, for whatever reason, it has the power to increase prices without constraint by competitors. A large market share or significant barriers to new entry into the market may be indicative of substantial market power. WM should consider this prohibition whenever its share of a market or market segment may exceed 40%.

Even in markets where WM has market power, it is entirely permissible to compete openly and fairly for business. WM remains free to price its products and services competitively and to enjoy the benefits of competitive advantages that result from such things as a better product, efficiency, innovation and expertise. However, in any market where WM has market power, refusals to do business with any person with the purpose of hurting a competitor may be illegal.

Similarly, the use of market power relating to one product or service to restrict competition in respect of another product or service may also breach the Commerce Act. For example, a refusal to sell one service to a customer unless it also buys some other service may be a breach if the service provider has market power in respect of the first service.

There is currently a Bill before Parliament to amend this prohibition. The new provision would prohibit firms with substantial market power from engaging in any conduct that has the purpose, effect or likely effect of substantially lessening competition in a market. This is seen as a lowering of the standard and will make it easier for the NZCC to successfully bring cases against dominant firms. It is therefore important that WM is aware that its obligations under this provision may change if this Bill is passed.

9.1 Predatory Pricing

In general, predatory pricing occurs when a company with market power cuts its prices below cost with the purpose of eliminating a competitor, restricting entry by a new competitor or preventing or deterring someone from engaging in competitive conduct.

No employee should offer or charge a price that he or she believes may be below WM's cost of providing the product or service without first obtaining advice from the Head of Legal.

10.0 Anti-Competitive Arrangements

The Commerce Act prohibits any contract, arrangement or understanding that has the purpose or likely effect of substantially *lessening competition*.

Whether an arrangement substantially lessens competition may not be immediately obvious. Employees should obtain advice from the Legal Team before entering into or giving effect to any contract, arrangement or understanding which has the potential to substantially lessen competition.

The formation of a joint venture between competitors can breach the Commerce Act if it is done with the purpose of or has the effect of substantially lessening competition. Other examples of arrangements which may, in some circumstances, substantially lessen competition include boycotts and exclusive dealing.

10.1 Exclusive Dealing

- a) The Commerce Act prohibits exclusive dealing arrangements with the purpose, effect or likely effect of substantially lessening competition. Exclusive dealing arrangements need not just be between competitors. It is illegal for a supplier and customer to enter into an exclusive dealing arrangement if it is intended to or does substantially lessen competition.
- b) Supplying goods or services to a customer on the condition that the customer does not do business with a competitor of WM can constitute exclusive dealing. So, too, can purchasing from a supplier on the condition that it does not sell to a competitor of WM. Refusing to trade with a customer or supplier because it has done business with a competitor of WM, or threatening to refuse to trade if the customer or supplier does business with a competitor can also breach the Commerce Act.
- c) Exclusive distribution or supply agreements are quite common but breach the Commerce Act if

they have the purpose, effect or likely effect of substantially lessening competition. To determine whether a contract is likely to “substantially lessen competition” within the meaning of the Act, it is often necessary to carry out a complex legal and economic analysis. Therefore, any contract that includes an exclusive dealing provision should be reviewed by the Legal Team before signing.

10.2 Boycotting or Exclusionary Provisions

An exclusionary provision is one that prevents, restricts or limits the supply or acquisition of goods or services from or to particular parties (e.g., boycotting a supplier or customer). If such a boycott has the purpose, effect or likely effect of substantially lessening competition, it will be a breach of the Commerce Act.

Employees should obtain advice from the Legal Team before entering into or giving effect to any contract, arrangement or understanding which contains an exclusionary provision.

11.0 Resale Price Maintenance

It is a common practice for manufacturers or distributors of goods to establish a recommended resale price when selling those goods to a reseller. This practice is perfectly legal if it is truly only a recommendation. The Commerce Act does not permit a manufacturer or distributor to require a customer to comply with a recommended price. It is illegal for a supplier to refuse to deal with a customer, to charge that customer a higher price, or otherwise punish a customer for selling at a lower price. However, it is not illegal for a supplier to set a maximum price that its retailers can on-sell goods.

12.0 Misleading or Deceptive Conduct

WM and all of its employees must be honest and truthful in dealing with customers and suppliers. Misleading or deceptive conduct in trade, or making false representations, can breach the Fair Trading Act. A statement or representation, even if literally true, can breach the Fair Trading Act if, under all of the circumstances, the statement is likely to mislead. Similarly, silence or providing incomplete, albeit truthful, information can have a tendency to mislead. WM employees are expected, not only to avoid false statements and representations, but also to take care that the totality of the acts and statements of WM are *not* likely to deceive or mislead. WM employees should not assume third parties, and especially customers, understand all WM terminology or know as much about the industry as WM employees do.

It is particularly important when WM employees are presenting service agreements for signing by potential customers that nothing be said that could mislead the customer as to the nature of the document or its terms. Any question raised by the customer should be answered fully and truthfully. Employees must avoid, however, providing legal advice to customers.

12.1 Unsubstantiated Representations

WM and all of its employees must take care to ensure that any representations they make about WM's products and services can be substantiated before they are made. “Representations” are not just words or statements about products and services, but can include pictures, photographs and implications made by way of conduct as well.

A representation is “unsubstantiated” if the person making the representation does not, when the representation is made, have reasonable grounds for making the representation. Examples of Unsubstantiated Representations include representations that WM's products are “the most sustainable in New Zealand” or its prices are the “lowest in the country” when WM has no basis for making these claims. An example of an unsubstantiated service claim is “WM will pick up your bin within 5 working days of you placing a collection order”. This statement must be substantially true, meaning all of time except in exceptional circumstances caused by say an extreme weather or other natural event.

WM and its employees will not be liable for making Unsubstantiated Representations where the representation amounts to “puffery”. The term “puffery” is used to describe claims that are expressions of opinion, as opposed to statements of fact, and are so obviously exaggerated that they are unlikely to mislead anyone.

12.2 False or Misleading Representations

WM employees must not make False or Misleading Representations that WM's products or services are of a particular kind, standard, composition or quality, new or manufactured at a particular time, or sponsored, approved or endorsed by a particular third party. In addition, WM employees must not make any False or

Misleading representation about the price, necessity or place of origin of WM's products or services.

A representation is false or misleading if it is untrue or is likely to create a false impression in consumers' or suppliers' minds as to the quality, characteristics or value of WM's products and services. Silence can, in some circumstances, amount to a False or Misleading Representation, such as when WM has a duty to disclose a piece of relevant information or only reveals part of the information. Even where WM was not the author of a False or Misleading Representation, but still disseminated it to the public, it can still be liable.

If you are in doubt about the authenticity of any statements you intend to make, or any statements made by WM's suppliers, you should seek advice from the Legal Team.

13.0 Uninvited Direct Sales

WM employees are expected to comply with certain rules when engaging in Uninvited Direct Sales. These rules govern circumstances where salespeople approach customers uninvited at their home, workplace or via telephone, to sell goods or services, and the price is either unascertained or over \$100. These rules are set out in the Fair-Trading Act and relate to the negotiation, disclosure requirements, cancellation and enforcement of agreements made in this context. WM Employees conducting Uninvited Direct Sales must be certain that they are aware of their obligations and ensure any agreements arising out of these interactions are in the required form. If you are unsure, please seek advice from the Legal Team.

14.0 Unfair Contract Terms

The Fair-Trading Act's Unfair Contract Terms regime ("**UCT Regime**") prohibits WM from using terms in standard form consumer contracts that are unfair. Unfair Contract Terms are terms which:

- a) cause a significant imbalance in the parties' rights and obligations under the contract;
- b) are not reasonably necessary to protect WM's interests; and
- c) would cause detriment to the customer if they were enforced.

Currently, the UCT Regime only applies to standard form consumer contracts (i.e. agreements that customers sign up to without negotiating these with WM). However, it will be extended to apply to certain business-to-business contracts in the future as well.

If you are concerned about the fairness of any terms that you are using within any contracts, please seek advice from the Legal Team.

15.0 Anticompetitive Mergers and Acquisitions

In addition to the above, it is a breach of the Commerce Act to acquire shares or assets of another company if the likely effect would be to substantially lessen competition in the market. In considering whether a particular acquisition is permitted by the Commerce Act, the Commerce Commission commonly considers such factors as the number and size of competitors, the substitutability of other services or products, barriers to entry and the effect of the acquisition on competitors and consumers. It is imperative that legal advice be sought for any acquisition by WM.

16.0 Consequences of Breaching this Policy or the Acts

It is in the interest of both WM and individual employees to report any potential breaches of this Policy or the Acts to the Legal Team as soon as a person becomes aware of it.

Employees who do not comply with this Policy, the Commerce Act or the Fair Trading Act may be subject to disciplinary action up to and including dismissal from employment. Breaches of these Acts potentially expose WM and the employee to large fines, claims by injured parties to recover damages, and prosecution in circumstances of intentional cartel behaviour. In most cases, the company will not be permitted by law to pay or reimburse a fine imposed on or legal costs incurred by an employee in circumstances where he/she has been found to have breached the competition and consumer laws.

The maximum penalty under the Commerce Act that may be imposed on a company for each instance of anti-

competitive conduct is the greater of:

- a) \$10 million;
- b) If the illegal benefit gained by WM can be determined, an amount equal to three times the illegal benefit; or
- c) If the illegal benefit cannot be determined, an amount equal to 10% of WM's (and related companies) annual turnover in New Zealand.

The maximum penalty under the Commerce Act that may be assessed against an individual involved in such conduct is \$500,000.

Further, intentionally engaging in cartel conduct is not only illegal, but is also a criminal offence. Those responsible for making the decision to enter or give effect to a cartel provision risk up to seven years imprisonment. However, it is a defence to a criminal prosecution if the individual reasonably believed that one of the exceptions to cartel conduct applied provided that the belief is not based on ignorance of the law or a mistake. It is therefore important that individuals speak with the Legal Team before relying on any of the exceptions.

The maximum penalties for any one breach of the Fair-Trading Act are \$600,000 for a company and \$200,000 for an individual.

17.0 Reporting Non-compliance

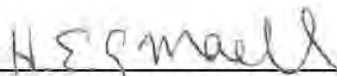
All employees are encouraged and obliged to report any actual or potential breaches of this Policy to WM's [Head of Legal](#).

WM may also conduct regular audits of employees' communications (including key word searches of employee email inboxes) to ensure compliance with this Policy.

18.0 Enquiries about this Policy

Any questions about the meaning of this Policy or about whether specific conduct is permissible under the policy should be directed to [WM Legal team](#).

This Policy will be reviewed as per date on footer.


Approved by the Managing Director
Date: 04 February 2022

Safe Driving Policy

1.0 Purpose and Scope

Waste Management NZ Limited (“WM”) will act to ensure the health and safety of its employees, contractors, customers and the general public through promoting professional driving and operating practices by its employees, contractors, subcontractors (“WM driver”) when operating WM owned and leased vehicles, plant and equipment, as well as any vehicle driven by a WM employee for work purposes including rental vehicles (“WM Vehicles”). This Policy outlines the responsibilities of WM and WM drivers in supporting this commitment.

2.0 Responsibilities of WM

WM shall:

- a) Provide Vehicles and procure rental vehicle plant and equipment, that are fit for purpose, are compliant with relevant safety and statutory requirements and are fitted with relevant safety and emergency equipment.
- b) Recognise that as a company, WM has a level of responsibility to ensure the safe use and operation of WM Vehicles.
- c) Ensure adequate resources are available to maintain a safe and compliant fleet.
- d) Provide driver assessments, training and information for all WM drivers as deemed necessary. This includes, but is not limited to:
 - i. Road safety training.
 - ii. Fuel efficiency training.
 - iii. Risk management.
 - iv. Specialised vehicle training.
 - v. Refresher courses or meetings.
 - vi. Advanced driver training (as required).
 - vii. Defensive Driving training.
 - viii. 4WD training (as required)
- e) Maintain records on WM driver training and competency in Vault at the Branch Level, as well as provide feedback to the driver.
- f) Investigate all reported incidents, infringements, near misses and hazards reported to WM and act in accordance with WM procedures.

3.0 Responsibilities of the WM Driver

3.1 Operating WM Vehicle

As applicable, each WM driver must:

- a) Complete all relevant training before being allowed to drive or operate plant and equipment unsupervised.
- b) Signed off on Risk Assessment for type of truck, or item of plant and equipment.
- c) Signed off on the Work Instruction or Coaching document for the type of truck, or plant and equipment
- d) Signed off and deemed competent to drive the truck or operate the item of plant or equipment unsupervised.

- e) Never drive or operate plant and equipment you have not been trained on
- f) Ensure the security of any WM Vehicles, plant, or equipment under their control by locking it when leaving the WM Vehicle unattended.
- g) Operate all WM Vehicles in a professional and courteous manner as ambassadors of WM and the WM brand.
- h) Operate all WM Vehicles, plant, and equipment in a safe manner and in accordance with prescribed operating procedures and all relevant safety and statutory requirements and obligations. This includes, but is not limited to:
 - i. Ensure this Policy has been read in conjunction with any other WM Policies.
 - ii. Maintain full compliance with all New Zealand Road Traffic Rules.
 - iii. Be in full control of the WM Vehicle at all appropriate times.
 - iv. Minimise distractions whilst driving.
 - v. Comply with company Standard Operating Procedures and work instructions (such as the Traffic Management Plans or other).
 - vi. Comply with operation Procedures as per any relevant NZTA or Worksafe NZ Code of Practice.
 - vii. Wear seatbelts at all times when driving or operating any item of plant where a seatbelt is fitted. Exception to this rule is granted if a driver is in the standing position operating from the left-hand side in a LEV, or when operating on an item of plant close to water.
 - viii. Prevent fatigue by allowing time for meal breaks and rests, making sure correcting lenses are worn if required, sunglasses are worn in bright weather, windscreens are kept clean, the inside of the WM vehicle is maintained at a moderate temperature, drinking plenty of water and stopping every two to three hours for a break.
 - ix. Ensure that in cab technology or mobile phones, are not used whilst the WM Vehicle is moving, and they are stored correctly while the WM Vehicle is in operation
 - x. Ensure children (being young person's 15 years of age or younger) are not in any WM Vehicle while being used for WM business, for reasons of safety. Should the need to transport child / children while undertaking WM operations, prior approval from the branch or division manager must be obtained in writing, stating the period of time for which such approval is given.
- i) No unauthorised person/s are allowed to operate or be transported in any heavy WM Vehicles or items of plant, unless authorised by the reporting manager.

3.2 NZTA (Waka Kotahi) Worktime Logbook Requirements

- a) Any worker driving a vehicle classified as a Class 2, Class 3, Class 4, or Class 5 must follow and abide by the below points at all times. Failure to do so could result in personal prosecution, fines, loss of licence and/or potential disciplinary.
 - i. Complete a logbook and abide by the New Zealand Worktime Logbook Rules at all times while driving any class 2, 3, 4, or 5 vehicles.
 - ii. WM requires all Class 2 drivers to complete a logbook and abide by the worktime/logbook rules even if operating within 50-kilometre radius of the work site.
 - iii. Workshop personal are exempt from completing a logbook if taking a truck for a service, COF (in the vicinity of the testing station) or conducting a road test within 50 kms radius from base where a load is not carried for hire or reward.
 - iv. Employees identified as having continuous logbook compliance issues or having been identified as not complying with the worktime & logbook rules will be required to undergo remedial training provided by WM and or may be subject to an investigation and disciplinary action.
 - v. Take a minimum 30 minute break before 5½ of driving time.
- b) Where a worktime rule breach occurs, the following disciplinary guidelines are to be followed

- i. Up to 5 breaches in any given month. For first time offence, employees will undergo further training and coaching. Should breaches continue then disciplinary action may be taken
 - ii. More than 5 and below 10 breaches in any given month. For first time offence, employees will undergo further training and coaching, and a formal discussion. Should breaches continue, disciplinary action will be taken
 - iii. More than 10 breaches in any given month may result in disciplinary action.
 - iv. Any severe breach of worktime rules may result in instant dismissal.
- c) Where secondary employment is undertaken that requires a logbook to be used, or results in worked hours impacting worktime rules i.e. a person drives during the week and is required to maintain a logbook, and then works a local store serving customers at a weekend. WMNZ must be informed to ensure there is no conflict of interest, the hours being worked do not impact your employment with WMNZ, and that fatigue is being managed to ensure rest periods required under worktime rules are being adhered to.

3.3 Monitoring and Reporting

Each WM driver must, as applicable:

- a) Conduct pre and post operation inspections of all heavy WM Vehicles, or any required WM Vehicle and record it through the daily driver's inspection and the WM Vehicle Condition Report (VCR) book, to determine that no damage or malfunction is evident that would affect the safe operation of the WM Vehicle. Light WM Vehicles will be inspected quarterly as per the WM Vehicle Policy and WM drivers must record weekly VCRs for the WM owned components of their WM Vehicles.
- b) Immediately report any damage or malfunction to a WM Vehicle to their direct manager. Failing to identify or report any damage before use makes the driver personally responsible for damage upon taking control of the WM Vehicle and/or plant and equipment.
- c) Immediately report any accident or incident that they are involved into their direct manager, regardless of the perceived / actual damage cost (if any) or severity of the incident, which,
 - i. Resulted in any WM Vehicle and/or plant and equipment under their control being damaged,
 - ii. Resulted in any other property damage, altercation, or injury; or
 - iii. Resulted in a near miss.
- d) In the event of an accident involving a WM Vehicle, weather at fault or not, and whether the WM Vehicle was being used for a business purpose or not, an employee must immediately contact their manager and submit themselves for a post-incident drug and alcohol test as soon as possible. This could be in addition to any testing undertaken by Police.

3.4 Incident and Infringement Notices

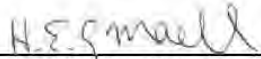
- a) A WM driver must report any incident, infringement notice or fine incurred while using a WM Vehicle during or outside of work activities as soon as practicable to their direct manager.
- b) Where WM receives notice of an infringement or fine, the WM driver responsible must give compensation to WM, by making immediate arrangements with their direct manager for the direct settlement of costs involved or payment of any debt to WM.
- c) An employee must co-operate fully in any investigation following any incident or infringement. Where an employee breaches road traffic rules or WM policies, an investigation and disciplinary action may result.
- d) In the event of a speeding incident (whether resulting in an infringement notice or recorded on a WM Global Positioning System ("GPS") device), the following guidelines apply in relation to disciplinary action:
 - 0 - 20% above the legal speed limit – for first time offence, may result in a written warning. Repeat offending may result in final warning.
 - 20 - 30% above the legal speed limit – may result in a final written warning.
 - Greater than 30% above the legal speed limit – potential dismissal.

- e) For other driving offences involving employees, such as running a red light or reckless driving – disciplinary outcome including potential dismissal.
- f) WM driver retraining/defensive driving may be enforced as applicable. See Section 3.4

3.5 Licenses and Training

- a) When driving a WM Vehicle on a public road, the WM driver must at all times hold, and be able to produce the required valid full licenses for the task being undertaken, including any endorsements, certificates or accreditations required for the task.
- b) If undergoing license development, they must hold the correct learners or restricted license (e.g. Class 2L, 4L and 5L) while undergoing training. Restricted licence holders must have gained permission to operate from the 'Head of People and Culture'. WM needs to ensure if permission is given, that the restricted licence moves to full licence within a short period of time six (6) months. WM will utilise the NZTA TORO system to verify the status.
- c) Consideration will be given to learner's license holders and valid overseas licenses holders. An overseas license is legally valid only if the license is written or translated correctly into English and the driver has been in New Zealand less than 12 months. Refer rules - NZ Transport Agency for new residents
- d) Where applicable licenses, certificates or accreditations either expire or are suspended, the WM driver must immediately notify their direct manager of such circumstances and not operate motor WM Vehicles until they have the regained applicable, current and valid license, certificate or accreditation. WM may apply mandatory revision training timetables to any certificate or accreditation that is not subject to expiry dates.
- e) All WM drivers must participate in Driver Assessment and Training, and any additional training as required by WM. WM drivers are required to follow any recommendations made by the training provider and confirm that they have understood any recommendations from the trainer.
- f) A WM driver may be required to participate in remedial driver training as per the WM-HR-P-12 Vehicle Policy.
- g) Where activities are undertaken at a WM controlled site that restricts unauthorised public access, WM drivers are excluded from the above license or endorsement requirements while progressing their license development. The WM driver or mobile plant operator MUST have undergone training on the relevant risk assessment/s, work instruction/s, and have been assessed and deemed competent, and capable to perform the task before being allowed to undertake a task unsupervised.
- h) The Site Manager MUST sign off the training forms and give authorisation before any unlicensed worker is allowed to operate, or drive any WM Vehicle, and ensure a detailed licence development programme has been implemented. If the WM driver has any questions regarding these rules, they should contact their direct manager in the first instance. Any breach of these rules may result in disciplinary action being taken.

This Policy will be reviewed as per footer.


 Approved by the Managing Director
 Date: 08 August 2023

Acceptable Use of ICT Policy (Under Review)

1.0 Objective

The Purpose of this Policy document is to outline the behaviours expected within Waste Management NZ Ltd ('WM') to protect ourselves, our company and most importantly our customers.

WM allow limited personal use of corporate devices while you are working; in return we must all commit to abiding by these requirements.

The use of Information and Communications Technology ("ICT") is crucial to the success of WM.

The key objectives of this Policy are:

- 1.1 To ensure employees understand how to use WM ICT in a safe, acceptable way, to minimise risk;
- 1.2 To prevent the compromise of WM ICT systems or loss of WM information;
- 1.3 To protect the privacy and confidentiality of client and business data held by WM;
- 1.4 To prevent data from being stored insecurely on a device or carried over an insecure network, where it can potentially be accessed by third parties.

2.0 Audience

The audience of this Detailed Requirements document includes everyone who has access to WM data, including employees, contractors, consultants and suppliers. Terms are marked in bold where a definition is provided at the end of the Policy.

3.0 Responsibilities

General policy related roles and implementation responsibilities for relevant stakeholders are defined within the ICT Security Policy.

4.0 Definitions

Anti-malware: a type of software program designed to prevent, detect and remove any malicious software (malware) on systems and devices.

e-Discovery: activities to discover digitally or electronically stored information, normally in support of an investigation into potential wrongdoing.

Jailbroken Device: a device that has been modified to remove restrictions imposed by the manufacturer or operator.

Personal Data: any information relating to an identified or identifiable natural person, e.g. date of birth, health data, network traffic data, content of communications, political preferences.

Phishing: the practice of sending messages pretending to be from reputable sources, in order to mislead individuals to reveal personal or sensitive information.

Virtual Private Network (VPN): an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted and prevents unauthorised eavesdropping on the traffic.

5.0 Scope

This Policy applies to all WM employees, contractors, consultants, visitors and suppliers who have access to WM ICT systems and resources, even if not via WM supplied and approved equipment.

Failure to comply with the Policy may result in the suspension of any and all technology use and connectivity or disciplinary action with possible termination of employment. People Services will be responsible for disciplinary action, in conjunction with the immediate manager, Head of ICT and CFO.

6.0 Responsibilities

- 6.1 The ICT department is responsible for implementing security measures and centrally managing security networks, applications, and data access. Any attempt to bypass security measures will be considered an intrusion attempt and will be dealt with by the ICT Department and may result in disciplinary action.
- 6.2 Staff are responsible for the security of data, accounts, and systems under their control. Passwords must be kept secure and should not be shared with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure access, is a violation of this Policy. Sharing a password with the ICT Department for support purposes is exempt and requires a change of password immediately after. If you suspect that one of your accounts or passwords has been compromised, then report this to the ICT Department immediately.
- 6.3 All WM owned equipment/devices should be cared for in a responsible manner. Any damage, loss or theft of equipment/devices must be reported immediately to your Manager.
- 6.4 The use of WM information systems, services and devices must be appropriate for its intended purpose and consistent with the WM Code of Conduct and the professional standards expected of WM employees.
- 6.5 All information and data on the WM system belongs to WM. Malicious deletion and theft of information/ data is considered a violation of Policy and will result in disciplinary action.
- 6.6 All internal and external activity on the WM network is logged; including email, messaging and external communications. WM may monitor the usage of all WM mobile devices and access all device information, including usage and websites visited.

IDENTITIES & PASSWORDS

WHY: To make sure that we all take accountability for our actions, and don't let malicious actors gain access to things they shouldn't.

Do...

- ✓ Act responsibly when using company-issued user identities and authentication credentials (e.g. passwords, PINs).
- ✓ Use a strong password that is not predictable or easily guessed.
- ✓ Change your passwords immediately if you suspect that anyone else might know them and report this to ICT Department immediately.
- ✓ Use approved password managers to store passwords.

Don't...

- ⊗ Use credentials that do not belong to you.
- ⊗ Allow anyone else to see or have access to your passwords, for example by writing them down or allowing someone to watch over your shoulder.
- ⊗ Re-use passwords that you use for WM systems for personal use, and vice versa.
- ⊗ Share passwords with colleagues to circumvent access controls.

SECURING INFORMATION

WHY: To protect information from being disclosed to people who shouldn't have access to it, and to make sure that the level of protection reflects how important the information is to WM

Do...

- ✓ Use storage media or resources that have been approved by ICT.
- ✓ Only use approved file transfer services, e.g. OneDrive, Dropbox
- ✓ Collect sensitive information from printers promptly.
- ✓ Dispose of sensitive information securely by shredding it or otherwise destroying it with approved methods.
- ✓ Access sensitive information within a secure environment and ensure you are not being over-looked.
- ✓ Back up information using approved solutions provided by ICT

Don't...

- ⊗ Use social media, collaboration platforms and other messaging tools (e.g. WhatsApp) for sensitive business information unless they are approved for business use.
- ⊗ Leave sensitive information, media or devices unsecured or in view when unattended.
- ⊗ Share sensitive information (i.e. payroll data) with anyone who is not authorised to view it.
- ⊗ Send sensitive information to third parties without first obtaining approval from the owner of the information.
- ⊗ Use free online services (translation, word graphic creation etc.) for processing sensitive information.

EMAIL

WHY: Malicious emails are one of the main ways that threat actors attempt to compromise WM, and one of the most common ways that sensitive information is accidentally leaked.

Do...

- ✓ Carefully check any emails that you are not expecting, and make sure not to open any links or attachments unless you know they are legitimate.
- ✓ Check suspicious emails for these typical signs of **phishing**:
 - a sender who is not known to you
 - requests for sensitive information such as usernames and passwords, financial details, and personal data
 - threats of negative consequences if you do not respond to the email, e.g. loss of access, escalation to management
 - lack of fluency, accurate spelling or correct grammar
 - embedded links or files that you are directed to open
 - invalid sender email that is trying to emulate a valid email address or individual within WM (e.g. firstname.secondname@Wastemanagement.gmail.com)
- ✓ Report any suspicious emails using the Report Message function in Outlook or send the email as an attachment to ICT Service Desk

Don't...

- ⊗ Include any sensitive information on external Out of Office messages.
- ⊗ Use company systems to send uninvited or spam email.
- ⊗ Use any personal email accounts for work purposes or forward any WM information to personal email accounts.
- ⊗ Use work-issued email addresses for personal reasons or non-work-related purposes, such as online shopping or running a personal business. This will reduce the threat of **phishing** emails that resemble expected communications.
- ⊗ Send any Credit Card data by any end user messaging technologies i.e., Email, Teams. If there is a valid business case the data must first be encrypted.

ACCEPTABLE USE POLICY

COMMUNICATIONS AND SOCIAL MEDIA

WHY: WM's brand is one of our most valuable assets. We need to be careful that our actions don't compromise or damage it.

Do...

- ✓ Refer any requested interactions with external media (newspapers, radio/TV stations, online news etc.) to the Marketing and Communications team.
- ✓ Behave appropriately when using social media platforms, by:
 - not disclosing confidential WM information
 - showing respect for the company, and everyone you deal with
 - openly disclosing your identity if involved in a discussion about work
 - using strong privacy settings for your profiles, and only connecting with people you know

Don't...

- ⊘ Provide any WM-related statement or information to the media without prior approval.
- ⊘ Speak at an external event as a WM representative, without first obtaining approval for your presentation from the Marketing and Communications team

REMOTE ACCESS & REMOTE WORKING

WHY: Outside of the office, we don't benefit from the numerous security controls that protect company property. As such, we need to take extra steps to protect our equipment and information

Do...

- ✓ Follow all the same security policies and procedures that apply when working in the office.
- ✓ Authenticate to the approved **Virtual Private Network** solution before beginning work and accessing WM information or systems.
- ✓ Take precautions, to protect any WM assets that you take out of the office from theft, damage and misuse.

Don't...

- ⊘ Discuss sensitive business information in public places.
- ⊘ Provide sensitive information to strangers without first verifying their identity and their right to access that information.

INTERNET AND INTRANET

WHY: We allow limited personal use of company resources such as your laptop but using these resources inappropriately can expose you to cyber threats (e.g., malware) or severe damage to our reputation.

Do...

- ✓ Use company resources in a way that is compliant with the laws and regulations we are subject to, and which upholds the Corporate **Code of Conduct (If applicable)**

Don't...

- ⊘ Perform the following activities using company resources:
 - posting illegal or defamatory information
 - accessing content relating to pornography, weapons, illegal drugs or gambling
 - accessing racist, sexist, threatening, hateful or otherwise discriminatory or objectionable content
 - accessing or distributing political or religious material

- accessing information subject to copyright or other intellectual property rights restrictions (e.g. music, videos)
- ⊗ Visit the following Internet site types, unless approved in advance by the local security team:
 - advice on how to circumvent or disable security controls
 - advice on how to conduct cyber attacks
 - sites providing unauthorised access keys, malware or compromised software
 - anonymous proxy servers
- ⊗ Internet use of a nature that consumes bandwidth at an unacceptable rate is specifically prohibited when there is no clear business-related use.
 - Examples include:
 - streaming services such as Netflix, Amazon Prime, Vodafone TV, Sky Go and Spark Sport;
 - illegal downloading of music, video or software;
 - playing games online.

SYSTEMS SECURITY

WHY: ICT Department has implemented a variety of controls to protect our systems from accidental or malicious damage. Attempting to disrupt or circumvent these controls could compromise our security and could constitute serious misconduct.

Do...

- ✓ Report any suspected malware infection to the ICT Service Desk immediately. Make no attempt to eradicate the malware or attempt to re-configure **anti-malware** tools.
- ✓ Use authorised access control mechanisms, and never attempt to circumvent these mechanisms.
- ✓ Use approved remote access solutions such as the **Virtual Private Network (VPN)** solution when connecting to the Internet from outside of the corporate network.
- ✓ Understand that all access to WM systems and resources will be logged and monitored by ICT Department.

Don't...

- ⊗ Import or activate any computer code designed to self-replicate, perform malicious activities, or degrade the performance of WM assets.
- ⊗ Use any computer program or process that consumes system resources to the extent that it interferes with business activities.
- ⊗ Establish any external network connections that allow unauthorised users to gain access to our assets.
- ⊗ Use WM systems to:
 - gain unauthorised access to other systems or information
 - damage, alter or disrupt the operations of other systems
 - obtain passwords, encryption keys or other access control credentials that could enable unauthorised access

ACCEPTABLE USE OF IT POLICY

WM OWNED EQUIPMENT

WHY: The technology we use every day to our jobs is vital to our business but is also a key target for attackers wishing to steal our information assets. It is therefore vital that we protect this equipment, and never compromise the controls in place to do so.

Do...

- ✓ Protect portable and mobile computing equipment from theft, unauthorised access or compromise.
- ✓ Only access WM information on mobile devices if you are using approved Mobile Device Management (MDM) solution.
- ✓ Return issued equipment and accessories at the end of your employment.

Don't...

- ⊗ Attempt to disable **anti-malware** and other security protection on corporate devices.
- ⊗ Leave WM devices unattended without logging out or activating a password-protected screen saver.
- ⊗ Lend a WM device meant for individual use, to any other individual.
- ⊗ Install any software on a company device that is not pre-approved business application.

USER OWNED DEVICES

WHY: 'Bring Your Own Device' initiatives give great flexibility and choice to users, but we need to be able to protect company information just as effectively on these devices.

Do...

- ✓ Accept that WM's security policy will be enforced on your device through Mobile Device Management (MDM).
- ✓ Accept that WM will not contribute towards the costs of BYO devices or personal SIM cards.
- ✓ Grant WM IT the ability to install management and security software (MDM)
- ✓ Report the loss of devices which access or store our data as soon as the loss has been discovered.
- ✓ Hand over the device and necessary access credentials, in the unlikely event that we need access to the device for e-discovery purposes.
- ✓ Remove all work information from personal devices when you leave employment with us.

Don't...

- ⊗ Use personal laptop computers to access WM resources, only mobile devices can be used as part of BYO policy.
- ⊗ Use **jailbroken** devices for business purposes.
- ⊗ Attempt to circumvent security controls used to protect WM information on the device.
- ⊗ Use unapproved personal solutions to back up corporate data, or back up corporate data along with any personal information stored on the device.
- ⊗ Use the device for illegal or unlawful purposes. This includes, but is not limited to intentional copyright infringements, software license infringements, obscenity, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation and computer tampering (e.g. spreading computer viruses or destruction of data owned by others).

N.B. WM will never access personal information from user owned devices or make it available to third parties there is a legitimate civil or criminal e-discovery request, or the user has explicitly authorised this access.

7.0 Document Control

The master version of this policy document shall be stored within the Policy Portal. Any other versions outside of that library location will be of an uncontrolled status.

8.0 Compliance

All use must comply with all applicable laws which include but is not limited to:

Privacy Act 2020;

Fair Trading Act 1986;

Copyright Act 1994;

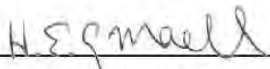
Defamation Act 1992;

Films, Videos, and Publications Classification Act 1993;

Unsolicited Electronic Messages Act 2007;

as well as any advertising codes of practice which may be relevant.

This Policy will be reviewed annually.


Approved by the Managing Director

Date: 18 November 2022

ICT Security Policy

1. Objective

The use of secure Information and Communications Technology ("ICT") is crucial to the success of Waste Management NZ Ltd ("WM").

The objective of this Policy is to

- ensure that all staff are aware of WM standards and processes for maintaining a secure ICT environment.
- protect our customers and business from Cyber risks including data breaches or unavailability of services, and the resulting financial, reputational, and legal consequences.

2. Scope

This Policy applies to

- **Services** – all WM internal functions and services, as well as customer facing services.
- **People** - all WM employees, contractors and visitors using devices, hardware, and related software to access WM ICT resources, even if this equipment is not approved, owned, or supplied by WM.

Not in Scope

- **Vendors:** Vendors providing services but without direct access to WM's systems, data and resources must adhere to Vendor specific policies or contractual terms.
- **Policy monitoring:** The Policy Owner is accountable for monitoring policy implementation.
- **Policy implementation:** The Policy Owner is accountable for the implementation of Information Security controls.

Compliance levels are monitored and reviewed by appropriate governance bodies. Failure to comply with the Policy may result in the suspension of any and all technology use and connectivity or disciplinary action with possible termination of employment. People Services will be responsible for disciplinary action, in conjunction with the immediate manager and CDO – Chief Digital Officer.

3. Policy Principles

The ICT Security Policy is the overarching security policy and sets the foundations for all other security policies and standards.

We are all responsible for protecting WM and our customers from cyber and information security risks. Everyone at WM (regardless of role or worker type) must do the right thing by following these principles and Behaviours:

PRINCIPLES	POLICY / STANDARD
<p>WM allows reasonable and legal personal use of company devices (PCs and phones). When you use these devices, you must follow the Acceptable use of ICT Policy.</p> <p>Follow the Do's and Don'ts regarding WM's information and equipment in order to protect ourselves, our company and most importantly our customers. Acceptable</p> <p>Usage of WM assets by our people is the most fundamental protection we have from information security risks.</p>	<p>Acceptable Use of ICT Policy</p>

PRINCIPLES	POLICY / STANDARD
Make sure that all of the WM workforces only have access to the information and assets required in order to perform their roles. All access to our data centers, hub rooms and IT cabinets is authorised.	Access Control Policy
Ensure passwords are kept confidential and are not shared or used by anyone else. Ensure the password policy is complied with for all passwords to WM systems and resources. Ensure passwords meet best practice	Password Management Policy
Remote access is only permitted through approved ICT services with appropriate approvals.	Remote Access Policy
Report any suspected malicious or Unauthorised activity through the ICT Service Desk so this can be managed and remediated.	ICT Incident Management Process
If you are responsible for owning, designing, or maintaining applications or infrastructure: <ul style="list-style-type: none"> - Capture and monitor activity logs to identify malicious or unauthorised behaviour. - Identify and remediate any vulnerabilities in our systems and technology. - Apply patches to remediate vulnerabilities and keep software up to date. - Configure systems securely, including hardening or installing anti-malware tools. - Secure the connections between systems, both internally and externally, to protect communications from Unauthorised access or modification. - All changes follow the ICT Change Management procedures - Hardware, software, and cloud-services are validated and approved by ICT Department before being installed and used. 	Logging & Monitoring Policy Patch Management Policy Network Security Testing Policy ICT Change Management Process
Identify, evaluate, and manage Cyber Security risks against WM's risk tolerance. Implement a program to assure Information Security controls and validate their effectiveness.	CIS Controls

The policy documents listed above outline the specific control requirements needed to implement these principles.

4. How Principles are implemented by WM ICT Security

To comply with this Policy, WM must take the following steps to identify and mitigate its specific security risks and comply with applicable legislation. These controls and activities can be delegated for efficiency purposes and must address both logical and physical security:

- Comply with all applicable legislation and regulation that may influence how we implement information security controls and processes.
- Implement the Cyber Security Strategy to direct how information cyber and security initiatives will be implemented in alignment with the local business priorities / strategy.
- Track and monitor security threats to WM's information, systems, and services.
- Confirm through formal security assessments that third parties such as suppliers meet minimum security requirements prior to connecting them to our internal networks and systems.

- Identify and prioritise the information, systems and services which are most important for the business and our customers and thus need to be protected from threats and related business risks.
- Utilise the WM's Risk Framework to identify the security risks to the business, to information and systems; understand the level of preparedness required to manage the risk; proactively measure and report on risks arising from non-compliance with the policy.
- Design, document, implement and operate controls that deliver the required level of protection
- Continually assess the design and operational effectiveness of the controls via assurance activities and processes, and accurately report control effectiveness.
- Implement a centralised cyber defense monitoring and surveillance capability.
- Respond to and recover from security incidents to minimise impact and disruption to the business and our customers.

5. Responsibilities

WM is committed to managing information security in a systematic way, in compliance with the principles of the international standard CIS Controls framework

The Policy Owner (CDO – Chief Digital Officer) is accountable for overseeing the implementation of the policy, including:

- the WM Cyber Security Strategy
- developing and maintaining the CIS Controls framework
- aggregating reporting on control effectiveness
- reviewing the policy on a planned or ad hoc basis for continuing suitability, adequacy and effectiveness and
- providing employees and contractors with the right security awareness, information, and training.
- Responding to cyber security incidents
- Complying with cyber and information security laws and regulations
- Aligning cyber security strategies, and
- Driving requirements and content for cyber security elements of the security awareness and training programme

Employees are required to:

- Be aware of and adhere to this Policy.
- Adhere to WM's [Acceptable Use of ICT Policy](#) at all times

The ICT department is responsible for

- implementing security measures and
- centrally managing security networks, applications, and data access.

Any attempt to bypass security measures will be considered an intrusion attempt and will be dealt with by the ICT department and may result in disciplinary action.

6. Exceptions to Policy

- The security principles are the mandatory minimum standard. If the principles cannot be fully implemented, the risk and impact must be assessed. Any risks that are High or Critical should be reported to the CDO – Chief Digital Officer.
- Approval for these risks will be provided by management based on the level of the risk in line with the WM Risk Framework. Low and Medium risks can be approved by the business owner, with the agreement of the CDO – Chief Digital Officer
- The Managing Director and CDO – Chief Digital Officer must approve all High and Critical risks.

7. Definitions

Assurance: An independent, objective assessment of the effectiveness of the controls being used to manage cyber and information security risk.

Availability: Information and services must be protected from deliberate or accidental loss, destruction, or interruption of services.

Compliance: Adhering to policies and standards. Essentially:

- (1) Know what to do: Implement Legal and regulatory requirements, policies, contracts and agreements
- (2) Build what is needed: Through Business and operations systems
- (3) Know what we have built: Documented through records, processes and controls
- (4) Check what we have done: Periodic reviews and comparisons between policy and reality
- (5) Say what we know: Through regular reporting

Information: Facts provided or learned about something or someone, e.g. customer account details, strategic plans, board meeting minutes.

Integrity: Information must be protected against unauthorised changes and modification.

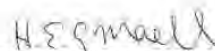
Logical Security: Software safeguards for an organisation's systems, including user identification and password access, authenticating, access rights and authority levels.

Physical Security: The capability of WM to ensure adequate measures are in place to safeguard personnel; to prevent or delay unauthorised access to assets; to detect attempted and actual unauthorised access and to activate appropriate responses.

Systems: Technology that is being used to process, transmit and store information and to provide services to our customers.

Risk: Something that can potentially affect WM's strategic & operational objectives. This may arise from something bad happening, or a failure of something good materialising.

This Policy will be reviewed annually.



Approved by Managing Director

Date: 09 May 2023

Environmental Policy

1.0 Objectives

At Waste Management NZ Limited and its subsidiaries ("WM") we are dedicated to providing environmentally beneficial and sustainable services, products and solutions to customers and the community that result in reduction, resource recovery, recycling and reuse of waste materials; efficient use of our own resources and conversion of waste to energy.

We are committed to achieving our aim of "Zero Harm" to the environment, and to continually improve our environmental standards for the benefit of the environment, our workers, stakeholders and the community.

We believe that the highest standards in environmental performance are crucial to the success and sustainability of our business.

2.0 WM Achieves these Objectives by:

- a) Developing ways to reduce, recover, recycle, or re-use waste in all aspects of our business, including considering and integrating environmental factors in our decision making process;
- b) Identifying opportunities for the prevention and reduction of pollution, including climate-modifying emissions, and implementing energy efficiency programs throughout the business;
- c) Providing resources to implement and maintain an effective system of environmental management;
- d) Identifying and understanding the environmental hazards inherent to the activities we undertake and effectively assessing, controlling and managing those risks;
- e) Complying with all legal requirements and standards applicable to our activities; and where adequate regulation does not exist, adopting practices that reflect our commitment to environmental compliance;
- f) Setting objectives, targets and key performance indicators which continually drive us to improve our environmental performance;
- g) Providing workers with training and information necessary for them to understand what the impacts of their activities are; and to enable them to work in an environmentally responsible and competent manner;
- h) Liaising, consulting and building relationships with our workers, regulators, local community and other key stakeholders to develop mutual respect for one another and the environment;
- i) Ensuring that incidents are investigated, specifically identifying the causal and contributing factors, so that remedial actions may be taken;
- j) Regularly undertaking audits and inspections of our operations;
- k) Communicating this Policy to workers and interested stakeholders; and reporting on our environmental performance openly and transparently;

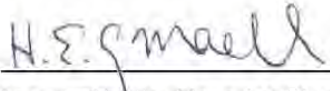
3.0 All Workers are required to:

- a) Carry out their work in accordance with WM's environmental policies, processes and procedures;
- b) Assess and manage the environmental hazards and risks associated with the activities they are undertaking; and
- c) Report any incident which generates any actual or potential harm to the environment.

4.0 Application

This Policy applies to all workers and joint venture partners engaged in activities under WM's operational control.

This Policy will be reviewed annually


Approved by the Managing Director
Date 14 November 2022

Dress Code Policy

1.0 Purpose

At Waste Management NZ Ltd ("WM") the way we present ourselves is important to maintain our professionalism and commitment to service. By looking presentable, we send a positive message to our customers, colleagues and the public. This Policy provides clear guidelines to our employees about how they are expected to present themselves. As WM employees work in a diverse range of environments, the Policy outlines the various levels of attire needed.

2.0 Operational Employees

- a) Operational employees are employees undertaking fieldwork activities for WM, who may be interacting with plant, machinery or equipment. All operational employees are required to wear PPE and equipment as directed by the [WM HSE PPE Guide](#).
- b) Employees may wear WM branded caps and beanies while working.
- c) Jewellery must not be worn in an operational environment where it isn't safely contained under the PPE clothing. This is to prevent an increased risk of accident or injury to the employee or others. WM will ensure that every attempt is made to support and enable the employee to work without discrimination or prejudice in their working environment.

3.0 Corporate and Office Bound Employees

- a) WM expects all employees to promote a clean and professional image to fellow staff, customers and the community. All corporate and office bound employees are expected to wear corporate clothing which reflects their role within WM i.e. minimum short sleeve, not strapless tops or singlets.
- b) WM allows employees to wear smart casual clothing (not street casual) on Fridays, provided that the employee complies with 4b) and does not have to attend any official meetings or represent the organisation to the public, clients or important external stakeholders.

4.0 Standards of Presentation

- a) All employees are expected to be well groomed and maintain a good standard of personal hygiene and appearance.
- b) For employees who aren't required to wear branded clothing in their role, must not wear unsuitable attire for the workplace. This includes beach or swim shorts, street casual t-shirts with offensive slogans, hoody sweatshirts and street wear sweatpants, night club street wear, ripped clothing and ripped jeans.
- c) Appropriate footwear, refer to [Section 7 – Footwear](#).

5.0 Wearing Traditional Community Attire

- a) We respect and celebrate the diversity of our workforce, including the wearing of traditional community attire. If an employee's religious or cultural beliefs through wearing traditional items, clothing and jewellery, is being discriminated against, they may consult with their [Business Partner - People and Culture](#) to ensure that they are supported in their work environment.
- b) Please ensure that in an operational environment, appropriate PPE must be worn over any traditional item to prevent an increased risk of accident or injury to the employee or others. WM will ensure that every attempt is made to support and enable the employee to work without discrimination or prejudice in their working environment.

6.0 Branded Clothing

- a) General Managers have the discretion to determine who is required to wear branded clothing in their region. Generally, this will be customer facing staff.
- b) WM will pay for required and voluntarily worn branded clothing.
- c) Employees and Managers are mutually responsible for ensuring the branded clothing is worn correctly.
- d) Employees not required to wear branded clothing have the option of receiving a portion of the branded clothing kit, at the discretion of their manager, paid for by WM, and to be worn at their discretion.
- e) For operational or customer facing roles, replacement of branded clothing will occur 12 months after issue, where old, branded clothing items will be traded in for new ones. If an item needs replacement before this time, the employee will notify their manager, who has the discretion to authorise an early replacement.
- f) Managers are responsible for tracking the branded clothing given to employees.
- g) Branded clothing will have logos at the discretion of WM, and employees may not obscure, alter or remove the logo from any branded clothing items.
- h) The laundering and maintenance of branded clothing is the responsibility of the employee.
- i) Branded clothing paid for by WM and any protective equipment provided by WM must be returned at the termination of employment.
- j) Employees who are required to wear branded clothing will be provided with:
 - i. Any combination of 3 shirts – business shirt / polos (shirts come with company logo)
 - ii. A jersey or vest
 - iii. A jacket (for roles that leave the office environment)
 - iv. A hat, cap or beanie (optional)
- k) Employees will not be provided with pants or skirts and may wear their own in compliance with this Policy.

7.0 Footwear


- a) For safety reasons, non-slip enclosed footwear will be desired to be worn at all times and be suitable for the work environment. Individual sites may have additional rules on what footwear must be worn on site, which the employee must comply with at all times.
- b) Good strong nonslip enclosed shoes, including good casual walking shoes are acceptable in the office environment.
- c) Customer facing i.e. sales staff, are expected to wear clean and tidy corporate appropriate footwear.
- d) Operational roles must wear appropriate PPE footwear related to their role.
- e) Loose footwear i.e. jandals, thongs, slip on Crocs and flip flops have safety issues and are not to be worn on any site.
- f) All visitors to the operational sites will be notified of the required footwear before they arrive at site.
- g) If any worker or visitor arrives at site without the correct footwear, the branch manager / supervisor must be informed immediately. The branch manager / supervisor will then either; provide the person with a pair of compliant shoes, ask the person to leave and return with compliant shoes, or for visitors, personally guide the person around the site as a managed risk.

8.0 Non-Compliance

- a) This Policy will be given to new starters in their induction, so they are clear on what is expected of them. Any changes to this Policy will be communicated throughout the business.

- b) Should any health / medical issues or disability result in the employee not being able to comply with any portion of this Policy, WM will ensure that every attempt is made to support and enable the employee to work without discrimination or prejudice in their working environment. They must engage with their immediate manager and consult with their [Business Partner - People and Culture](#) to ensure that they are supported in their work environment.
- c) Where an employee is wearing inappropriate attire to work, the manager will privately discuss this with the employee, and the employee is expected not to wear the same inappropriate attire again. If the employee continues to wear inappropriate attire, the matter will become a performance issue and may be subject to disciplinary action.
- d) Any questions related to the content of this Policy or its interpretation should be directed to your region's [Business Partner - People and Culture](#).

This Policy will be reviewed as per the date of the footer



Approved by Managing Director

Date: 10 March 2023