

Whistleblower Policy

Last Updated: October 2026

1. Introduction

This Policy applies to the following More Group of companies ("**More**" or the "**More Group**"):

- More Telecom Pty Ltd
- Tangerine Telecom Pty Ltd

The More Group is committed to operating legally, properly, and ethically, and creating a transparent and open environment where people feel comfortable raising concerns.

This Policy is a small step in supporting this mission, and sets out the protections available to whistleblowers, what matters are reportable, how you can report your concerns without fear of backlash, and how the More Group will support and protect you.

How to make a report	
Report by email	wpo@more.com.au or wpo@tangerinetelecom.com.au
Report online	More whistleblower reporting form or Tangerine whistleblower reporting form
Who receives the report	The Whistleblower Protection Officer—currently the Chief Legal Officer or, in their absence, the Head of Legal.
Your options	You may report anonymously or use a pseudonym. Internal reporting is encouraged but is not mandatory. Section 4 explains all reporting options and the information that may assist More Group to respond.

2. Scope

This Policy applies to More Telecom Pty Ltd and Tangerine Telecom Pty Ltd. Together, these companies are referred to in this Policy as "More Group". Section 3.1 identifies the people who may make a disclosure and qualify as eligible whistleblowers under the *Corporations Act 2001* (Cth).

A personal work-related grievance will not usually qualify for protection under the *Corporations Act 2001* (Cth) unless an exception applies. Some grievances may still be protected, including where they also involve broader misconduct, a breach of certain laws, a danger to the public, or detriment arising from a protected disclosure. Section 3.3 explains these exceptions. If a matter is solely a personal work-related grievance and no exception applies, More Group employees and contractors should refer to the More Grievance Procedure.

3. General Principles

3.1 Who is an “eligible whistleblower”?

An individual may make a disclosure and qualify as an “eligible whistleblower” under this Policy if they are, or have previously been:

- an officer or employee (e.g. current and former employees who are permanent, part-time, fixed-term or temporary, interns, secondees, managers, and Directors);
- a supplier of services or goods to the More Group (whether paid or unpaid), including their employees (e.g. current and former contractors, consultants, service providers and business partners);
- an associate of the More Group; and/or
- a relative, dependant or spouse of an individual set out above (e.g. relatives, dependants or spouse of current and former employees, contractors, consultants, service providers, suppliers and business partners).

To access the whistleblower protections described in this Policy, a person must fall within at least one of these statutory categories. This requirement also applies where a report is made anonymously.

3.2 Disclosable matters

A “disclosable matter” involves information that the discloser has reasonable grounds to suspect concerns misconduct, or an improper state of affairs or circumstances, in relation to More (or a related body corporate of More).

Examples of this may include:

- illegal conduct, such as theft, dealing in, or use of illicit drugs, violence or threatened violence, and criminal damage against property;
- fraud, money laundering or misappropriation of funds;
- offering or accepting a bribe;
- financial irregularities;
- failure to comply with, or breach of, legal or regulatory requirements;
- engaging in or threatening to engage in detrimental conduct against a person who has made a disclosure or is believed or suspected to have made, or be planning to make, a disclosure.

A disclosable matter may not involve a breach of a particular law. For example, information that indicates a significant risk to public safety or the stability of, or confidence in, the financial system is also a disclosable matter, even if it does not involve a breach of a particular law.

Finally, a discloser can still qualify for protection even if their disclosure turns out to be incorrect.

3.3 Personal work-related grievances

A personal work-related grievance will not usually qualify for protection under the Corporations Act if the information concerns the discloser personally and does not

have significant implications for More Group that extend beyond the discloser. Examples include:

- an interpersonal conflict between the discloser and another employee;
- a decision that does not involve a breach of workplace laws;
- a decision about the employment, engagement, transfer or promotion of the discloser;
- a decision about the terms and conditions of employment or engagement of the discloser;
- a decision to suspend or terminate the engagement of the discloser, or otherwise to discipline the discloser.

A personal work-related grievance may still qualify for protection where an exception under the Corporations Act applies, including if:

- it includes information about misconduct, or information about misconduct includes or is accompanied by a personal work-related grievance (mixed report);
- More has breached employment or other laws punishable by imprisonment for a period of 12 months or more, engaged in conduct that represents a danger to the public, or the disclosure relates to information that suggests misconduct beyond the discloser's personal circumstances;
- the discloser suffers from or is threatened with detriment for making a disclosure;
- the discloser seeks legal advice or legal representation about the operation of the whistleblower protections under the Corporations Act.

For personal work-related grievances, please refer to the More Grievance Procedure.

3.4 False reporting

A disclosure will not be considered false merely because it is not substantiated. A person who has reasonable grounds for their suspicion may make a disclosure even if the information later proves to be incorrect. However, a person must not knowingly provide false information under this Policy. A person found to have deliberately made a false report may face disciplinary action, up to and including termination of employment or engagement.

3.5 Who should disclosures be made to?

More Group encourages disclosable matters to be reported internally to the **Whistleblower Protection Officer** (currently the Chief Legal Officer or, in their absence, the Head of Legal) because this enables More Group to respond promptly. Internal reporting is not mandatory, and protection under the Corporations Act does not depend on first reporting to More Group.

The Whistleblower Protection Officer is tasked with:

- managing the disclosure process (including reporting, investigations and communicating outcomes to stakeholders);
- identifying risks to an eligible whistleblower within the organisation and the workplace; and

- putting in place appropriate measures to ensure eligible whistleblowers are protected from prohibited conduct by other members of the More community.

You may make a disclosure about a disclosable matter directly to another internal eligible recipient, certain regulators, or a legal practitioner and qualify for protection under the Corporations Act. You are not required to report internally before using these options.

An “eligible recipient” can be any of the following:

- any director, officer or senior manager of any More Group company;
- an internal or external auditor of any More Group company; or
- a person or third party service provider authorised by More to receive disclosures that may qualify for protection.

Disclosures to a legal practitioner for the purposes of obtaining legal advice or legal representation in relation to the operation of the whistleblower provisions in the Corporations Act are protected (even if the legal practitioner concludes that a disclosure does not relate to a ‘disclosable matter’).

Disclosures of information relating to disclosable matters can be made to ASIC, APRA or another Commonwealth body prescribed by regulation and qualify for protection under the Corporations Act.

3.6 Can you remain anonymous?

- **You may remain anonymous.** An eligible whistleblower may choose to remain anonymous when making a disclosure, during any investigation and after the investigation is finalised. They may also use a pseudonym and may refuse to answer questions that they believe could reveal their identity.
- **You may use the same reporting channels.** If you wish to remain anonymous, use any reporting method set out in this Policy and state that you do not want your identity disclosed (noting that if you choose to submit a report via email, your identity may be disclosed solely to the Whistleblower Protection Officer as a result). You may choose to remain anonymous even if you have previously identified yourself.
- **More Group will protect your identity.** More Group will keep a discloser’s identity confidential and will not disclose it except with the discloser’s consent or where disclosure is authorised or required by law. Information that may identify the discloser will be shared only where lawful and reasonably necessary for investigating the matter, and More Group will take reasonable steps to reduce the risk of identification. Anonymous reporting can limit More Group’s ability to investigate or provide feedback, so disclosers are encouraged, where possible, to maintain secure two-way communication for follow-up questions and updates.

3.7 Emergency disclosures

If you have reasonable grounds to believe that information you have reported concerns a substantial and imminent danger to the health or safety of any third party, or to the natural environment, you may consider making an “emergency disclosure” to a journalist or parliamentarian, provided that:

- you have first made a disclosure of the information to an authorised regulatory body (e.g. ASIC);
- before making the emergency disclosure, you have given written notice to the same regulatory body that:
 - includes sufficient information to identify the previous disclosure; and
 - states that you intend to make an emergency disclosure; and
- your disclosure must contain no more information than is necessary to inform the journalist or parliamentarian of the substantial and imminent danger.

We recommend you contact an independent legal adviser before making an emergency disclosure.

3.8 Public interest disclosures

If you have reasonable grounds to believe that the information you have reported is in the public interest, you may consider making a “public interest disclosure” to a journalist or parliamentarian, provided that:

- at least 90 days have passed since you made an initial disclosure to an authorised regulatory body (e.g. ASIC);
- you do not have reasonable grounds to believe that action is being, or has been taken, in relation to the disclosure,
- you have reasonable grounds to believe that making a further disclosure of the information is in the public interest; and
- before making the public interest disclosure, you have given written notice to the same regulatory body that:
 - includes sufficient information to identify the previous disclosure; and
 - states that you intend to make a public interest disclosure.

We recommend you contact an independent legal adviser before making a public interest disclosure.

4. How to make a whistleblower report

4.1 Reporting internally

A report can be made confidentially to the More Group Whistleblower Protection Officer by:

- sending an email to wpo@more.com.au or wpo@tangerinetelecom.com.au; or
- completing and submitting a report using the webform available at <https://www.more.com.au/whistleblower-reporting> or <https://www.tangerine.com.au/whistleblower-reporting>.

Alternatively, you can make a report directly to any other internal More Group eligible recipient using the contact details available for those individuals on More Group’s internal contact directory.

If you make a disclosure directly to another More Group eligible recipient, you are encouraged to document your concerns in writing and mark any email correspondence

“PRIVATE & CONFIDENTIAL”. These steps are helpful but are not required for a disclosure to be considered.

You should include as much information as possible about the alleged breach in your report so that it can be investigated, including:

- the nature of the alleged breach;
- the person or persons responsible for the alleged breach;
- the facts on which the eligible whistleblower’s belief, that a breach has occurred and has been committed by the person/s named, are founded; and
- the nature and whereabouts of any further evidence that would substantiate the eligible whistleblower’s allegations, if known.

The above disclosures can be made anonymously, confidentially, securely and outside of business hours.

4.2 Reporting externally

If you have chosen to make a protected disclosure to an applicable regulatory body, More requests that you consider also notifying More. This is not required, but it will assist More to ensure it is doing everything possible to support and assist you.

More may also nominate external persons to whom, or agencies to which, disclosures may be made under the protections offered under this Policy. Where such a nomination is made, employees will be informed by any appropriate method.

5. What happens after a disclosure is made?

More Group will manage each disclosure through the following stages. The process may be adapted to the nature and circumstances of the matter, while maintaining confidentiality, impartiality and procedural fairness.

Stage 1— Acknowledgement, initial contact and assessment

- where contact details are available, acknowledge the disclosure and explain the next steps;
- assess whether the disclosure may qualify for protection, identify any immediate risk of detriment, and implement appropriate interim safeguards;
- seek further information from the discloser where appropriate and assess whether the matter should be investigated or referred through another process; and
- notify the Board or a relevant director where appropriate, subject to confidentiality requirements.

Stage 2— Investigation decision, scope and appointment

If an investigation is warranted, More Group will appoint an appropriately skilled and impartial investigator, address any actual or perceived conflict of interest, and determine:

- the terms of the investigation;
- the nature and scope of the investigation;
- the person within or outside More Group who should lead the investigation, having regard to independence, expertise and conflicts of interest;

- the nature of any technical, financial or legal advice that may be required to support the investigation; and
- the timeframe for the investigation.
- if the disclosure does not meet the requirements of this Policy, or there is insufficient information to proceed, More Group may decide not to investigate further. Where lawful and practicable, More Group will explain that decision to the discloser.

Stage 3 — Investigation and procedural fairness.

The investigator will gather and assess relevant information objectively. A person whose conduct is the subject of investigation will be given a fair opportunity to respond to material allegations, where appropriate and subject to confidentiality and legal requirements.

Stage 4 — Updates, records and protection monitoring.

Where contact details are available, More Group will provide updates to the discloser at key stages, subject to confidentiality and legal constraints. More Group will maintain appropriate records, communicate securely and reassess the risk of detriment as the matter progresses and after it is closed.

Stage 5 — Findings, recommendations and closure.

At the conclusion of an investigation, the investigator will provide a report to the Whistleblower Protection Officer and, where appropriate, the Board or relevant directors. The report will set out findings, recommendations and any proposed corrective action. Where lawful and practicable, More Group will advise the discloser that the matter has been finalised and provide an appropriate summary of the outcome. The level of detail provided will depend on confidentiality, privacy and procedural fairness requirements.

6. Legal protections for whistleblowers

6.1 Overview of Protections

The Corporations Act provides the following legal protections to a discloser whose disclosure qualifies for protection:

- identity protection (confidentiality) (unless you give your consent to be identified or specific limited exceptions apply);
- protection from detrimental acts or omissions;
- compensation and other remedies; and
- civil, criminal and administrative liability protection.

6.2 Identity protection (confidentiality)

Legal protection. The Corporations Act restricts disclosure of a protected discloser's identity and information likely to identify them, except where the discloser consents or disclosure is authorised by law.

More Group safeguards. To support this legal protection, More Group will apply the following safeguards (where appropriate):

- all personal information or reference to the eligible whistleblower witnessing an event will be redacted;
- the eligible whistleblower will be referred to in a gender-neutral context;

- where possible, the eligible whistleblower will be contacted to help identify certain aspects of their disclosure that could inadvertently identify them;
- disclosures will only be handled and investigated by appropriate staff;
- all paper and electronic documents and other materials relating to disclosures will be stored securely;
- access to all information relating to a disclosure will be limited to those directly involved in managing and investigating the disclosure;
- only a restricted number of people who are directly involved in handling and investigating a disclosure will be made aware of a whistleblower's identity (subject to the whistleblower's consent) or information that is likely to lead to the identification of the whistleblower;
- communications and documents relating to the investigation of a disclosure will not be sent to an email address or to a printer that can be accessed by other staff; and
- each person who is involved in handling and investigating a disclosure will be reminded about their confidentiality obligations (including that an unauthorised disclosure of a whistleblower's identity may be a criminal offence).

6.3 Protection from detrimental acts or omissions

Legal protection. A person must not engage in conduct that causes detriment to a discloser or another person because they believe or suspect that the discloser or another person made, may have made, proposes to make or could make a disclosure that qualifies for protection. This protection applies where that belief or suspicion is the reason, or part of the reason, for the conduct.

In addition, a person cannot make a threat to cause detriment to a discloser (or another person) in relation to a disclosure. A threat may be express or implied, or conditional or unconditional. A discloser (or another person) who has been threatened in relation to a disclosure does not have to actually fear that the threat will be carried out.

Examples of detrimental conduct include dismissal of an employee, injury of an employee in their employment, alteration of an employee's position or duties to their disadvantage, discrimination, harassment or intimidation of a person, or damage to their property, reputation, business or financial position.

More Group safeguards. More Group will assess and control the risk of detriment to a discloser through the following steps:

- **Risk identification:** Assessing whether anyone may have a motive to cause detriment—information may be gathered from a discloser about:
 - the risk of their identity becoming known;
 - who they fear might cause detriment to them;
 - whether there are any existing conflicts or problems in the workplace; and
 - whether there have already been threats to cause detriment.
- **Risk analysis and evaluation:** Analysing and evaluating the likelihood of each risk and evaluating the severity of the consequences.
- **Risk control:** Developing and implementing strategies to prevent or contain the risks. For anonymous disclosures, More may assess whether the discloser's identity can be readily identified or may become apparent during an investigation and apply appropriate safeguards.

- **Risk monitoring:** Monitoring and reassessing the risk of detriment where required. The risk of detriment may increase or change as an investigation progresses, and even after an investigation is finalised.

Where appropriate, the CEO will designate an officer to be responsible for ensuring that the person suffers no employment-related disadvantage on account of their actions in this matter and for providing additional support where necessary.

6.4 Compensation and other remedies

A discloser (or any other employee or person) can seek compensation and other remedies through the courts if:

- they suffer loss, damage or injury because of a disclosure; and
- More failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

All individuals are encouraged to seek their own independent legal advice if they believe the above has occurred.

6.5 Civil, criminal and administrative liability protection

A discloser is protected from any of the following in relation to their disclosure:

- civil liability (e.g. any legal action against the discloser for breach of an employment contract, duty of confidentiality or another contractual obligation);
- criminal liability (e.g. attempted prosecution of the discloser for unlawfully releasing information, or other use of the disclosure against the discloser in a prosecution (other than for making a false disclosure)); and
- administrative liability (e.g. disciplinary action for making the disclosure).

However, the above protections do not mean that disclosers can't be held responsible for their own actions. For example, making a disclosure doesn't mean that More cannot take disciplinary action against you for any misconduct that you are found to have engaged in. The protections relate to the making of the disclosure itself, and not in relation to any information that it reveals about your behaviour.

7. **Responsibilities**

7.1 CEO

The CEO is responsible for:

- appointing the Whistleblower Protection Officer;
- receiving material notifications and reports under this Policy;
- ensuring appropriate action is taken in response to disclosures, investigation findings and recommendations;
- promoting compliance with this Policy; and
- reviewing this Policy annually with the Whistleblower Protection Officer, or earlier following a legislative or regulatory change, a material whistleblower matter, an identified control weakness, or a change to reporting channels or responsible officers.

7.2 Whistleblower Protection Officer

The Whistleblower Protection Officer is responsible for:

- administering this Policy and ensuring it remains accessible;
- receiving and assessing disclosures and explain the applicable process to disclosers;
- assessing and monitoring risks of detriment and arranging appropriate safeguards;
- appointing or overseeing impartial investigations, manage conflicts of interest and monitor corrective actions;
- maintaining appropriate confidential records;
- arranging appropriate training and promoting compliance with this Policy and applicable whistleblower laws; and
- reporting material matters to the CEO, Board or relevant directors, subject to confidentiality requirements.

7.3 More employees

All More employees are required to:

- be familiar with this Policy and complete required training;
- raise concerns about suspected serious misconduct, unlawful conduct or other disclosable matters using an appropriate reporting channel;
- maintain confidentiality and cooperate with investigations when requested; and
- not cause, threaten or tolerate detriment against a person because of an actual or suspected disclosure.

8. **Accessibility of this Policy**

More will take steps to ensure that this Policy is made available to More's officers and employees and is easily accessible. For example, More will:

- store this Policy in a central location where it can be accessed by all More Group team members at any time;
- incorporate this Policy into its online education and training program for More team members;
- display this Policy on its website, accompanied by a webform that enables confidential reporting; and
- carry out appropriate training and education for senior managers and officers.

9. **Breach of this Policy**

Any breach of this Policy may result in counselling and/or disciplinary action, up to and including termination of employment or cessation of engagement.

Employees must also acknowledge that a breach of this Policy may also constitute a breach of applicable legislation, which could result in legal or regulatory action (including criminal action and penalties), significant reputational damage and substantial financial loss.

Owner	More & Tangerine Chief Legal Officer
Effective Date	12/10/2026
Version Number	3
Next review date	11/10/2027