Dicker Data Limited
Whistleblower Policy

ABN 95 000 969 362

DICKER DATA

Table of Contents

1. Purpose and Scope

1.1 The Policy sets out the principles for making, receiving, investigating and addressing disclosures made by Whistleblowers (as defined in part 2 below). The Company believes every employee should have the chance to speak up anonymously when they feel we are not adhering to our corporate values or complying with the law. The Company believes everyone should be able to make disclosures anonymously. We protect Whistleblowers' identities and they only need to reveal their identity if they choose to. The Company provides Whistleblowers a place to report concerns and, after proper investigation based on the results, we commit to fixing problems and making improvements.

1.2 **It is important that Whistleblowers:**

a) are encouraged to express their concerns;

b) know how to express their concerns,

c) understand their right to remain anonymous if they choose;

d) understand what we will do if a matter is reported;

e) feel safe in expressing their concerns; and

f) understand that they will not be subject to retaliation or victimisation in response to expressing their concerns.

1.3 The Policy applies globally. It applies to all the Company's subsidiaries, businesses, divisions, and offices. It also applies across all jurisdictions where we operate. If local legislation, regulation, or laws provide a higher level of protection than what is included in this Policy, the local legislation, regulation or laws prevail.

1.4 The Policy does not form part of any contract of employment or any industrial instrument.

2. What is a Whistleblower?

2.1 A Whistleblower is an Eligible Person (as defined in part 2.2 below) who makes or attempts to make a disclosure of Reportable Conduct (as defined in part 2.3 below). The Whistleblower must refer to the Policy or request the protections under the Policy.

2.2 An Eligible Person means:

a) directors, officers, managers, employees (including part-time, casuals, interns etc.);

b) contractors, consultants, suppliers, service providers (or their employees or subcontractors);

c) auditors;

d) former employees of the Company; or

e) a relative or dependent of any of the above.

2.3 For the purpose of this Policy, Reportable Conduct means any conduct or an improper state of affairs which includes, but is not limited to:

a) dishonest;

b) fraudulent;

c) corrupt;

d) illegal;

e) breaches the law, a regulation or any legal code;

f) in serious breach of internal policy (including Dicker Data's Code of Conduct or policies);

g) unethical;

h) improper;

i) unlawfully discriminatory;

j) bullying and harassment;

k) creates an unsafe work environment; or

l) any other conduct which may cause us financial or non-financial loss (including reputational harm) or be otherwise detrimental to the interests of the Company.

3. Making the Disclosure

3.1 If an Eligible Person would like to make a disclosure, they have various channels available where they can do this. Detailed instructions for how to use and approach each of these channels are included in Dicker Data – Appendix 1.

3.2 The Whistleblower must act honestly and reasonably in making the disclosure, with a genuine belief that the Reportable Conduct has occurred.

4. Content of the Disclosure

4.1 A Whistleblower should consider providing as many of the following details as possible, to facilitate a full and fair investigation and assist in determining the best course of action:

a) the specific nature of the conduct or improper state of affairs that concerns you;

b) the details of the person you think engaged or is engaging in any relevant conduct;

c) when and where relevant events occurred (e.g. dates and times);

d) details of anyone else aware of or involved in the conduct or events;

e) details of anyone else who might be able to verify your disclosure;

f) if you have done anything in response to the conduct or events;

g) if you have any concerns about possibly being victimised, and if so by whom; and

h) any supporting information (e.g. documents, file notes, emails, photographs).

5. Anonymity and Confidentiality

5.1 The Company will make every effort to respect and protect the identity of a Whistleblower if they choose to make an anonymous disclosure or ask to place restrictions on who is informed of their disclosure. At any time, a Whistleblower can choose to identify themselves, but this is their choice and at no point do they need to do this nor will they be forced to provide their identity. If a Whistleblower decides to disclose their identity, then the Company will outline and document who in the organisation will know they submitted the disclosure. The Company will also take all reasonable steps necessary (outlined in this Policy below) to ensure the Whistleblower does not suffer any retaliation.

5.2 Although we will take all reasonable steps to reduce the risk that you will be identified as a result of a required disclosure, there are some limited situations where the Company may not be able to comply fully with a Whistleblower's request to remain anonymous. For example, where:

a) we are compelled by law to do so (for example, where the Company receives a valid subpoena);

b) there is an immediate and substantial risk to the health or wellbeing of a person (for example, where a disclosure suggests an employee might engage in self-harm or harm others);

c) we need to engage external legal counsel in order to obtain legal advice;

d) we use a specialist external investigator;

e) we consider we are obligated to make a disclosure to a regulator or the police under legislation (for example, where a felony has been reported we may be required to report it to the police); or

f) there is an imminent risk of serious harm or danger to public health or safety, or to the financial system, if the information is not acted on immediately.

5.3 Whilst we will still make best endeavours to investigate the disclosure, there may be some practical limitations in doing so if the Whistleblower does not agree to share their disclosure or identity. There may be limitations of what can be achieved if the Whistleblower decides to remain anonymous.

6. The Investigative Process

6.1 Once a Whistleblower disclosure is submitted (anonymous or not), this report goes to the General Manager People and Culture and, where appropriate, the General Counsel. The Company may investigate a Whistleblower disclosure internally or use third parties to investigate any disclosure. For example, the investigation might be conducted by General Counsel or external legal counsel, finance, an accounting firm, forensic accountants, forensic IT investigators, HR, external HR consultants or an external investigator with suitable skills in the relevant area. The investigation process may include:

a) initial assessment to confirm it is a valid Whistleblower disclosure;

b) informing the Board or unimplicated management personnel on a need to know basis;

c) undertaking an investigation which may include corresponding with the Whistleblower if there is a need to do this and the identity of the Whistleblower is known;

d) preparing an investigation report which will include findings of fact; and

e) providing an investigation report to appropriate company personnel (e.g. management) or the Board for any subsequent action to take place.

6.2 As part of our investigative process, the Company may update the Whistleblower, if applicable, of the progress of any investigation. The receipt of the disclosure will be confirmed to the Whistleblower and they will be informed when the investigation is commenced and when it is concluded. Additional progress reports may be provided to the Whistleblower during the investigation.

6.3 The Whistleblower will be provided with a high-level summary of the outcome of the investigation. Findings may be that an allegation is fully substantiated, partially substantiated, not able to be substantiated, or disproven. There may be information that cannot be shared with the Whistleblower.

6.4 If, after receiving the high-level summary of the investigation, the Whistleblower is not satisfied with the result, they can request the matter be escalated as appropriate. The Whistleblower must provide this escalation request in writing along with details as to the basis for the request. The appropriate escalation path will be determined on a case-by-case basis.

7. Anonymity After Submitting A Disclosure

7.1 We explained above how a Whistleblower can request to remain anonymous after submitting a disclosure and during any investigation. The following procedures apply to protect the identity of Whistleblowers:

a) the Whistleblower has the right to remain anonymous and does not need to identify themselves at any time during the investigation process;

b) the Company may use tools and platforms that help protect a Whistleblower's identity;

c) at no time will the Company force the Whistleblower to reveal their identity;

d) the Whistleblower can refuse to answer questions they feel could identify themselves;

e) if the Whistleblower reveals their identity at any time, we will document who will have access to their identity.

8. Retaliation Prohibited

8.1 We prohibit all forms of retaliation against a Whistleblower as a direct result of making a disclosure within the scope of the Policy or applicable legislation. We take all reasonable steps to protect Whistleblowers from any retaliation. This includes (but is not limited to) protection from:

a) termination of employment (unless unrelated and in the ordinary course of business),

b) disciplinary action;

c) performance management (unless in the ordinary course of business);

d) harassment or bullying;

e) personal or financial disadvantage;

f) unlawful discrimination; or

g) any other conduct that constitutes retaliation.

8.2 If the Whistleblower feels that they have been or will be retaliated against, they should escalate this immediately to the General Manager, People & Culture. The General Manager, People & Culture will take the action they feel is appropriate in order to address any valid concern.

8.3 If the Whistleblower feels their report of retaliation was not resolved adequately, they can escalate this case in writing to the CEO or the Board.

8.4 We may raise with a Whistleblower matters that arise in the ordinary course of their employment or engagement (e.g. separate performance or misconduct issues). We have discretion to grant a Whistleblower who has not engaged in serious or unlawful conduct, immunity from company disciplinary proceedings relating to matters that come to light as a result of their disclosure. These protections are designed to encourage people to disclose unlawful, improper or unethical behaviour to relevant parties. We also seek to protect people who are witnesses or otherwise involved in investigating disclosures from retaliation arising their provision of evidence to or involvement in that investigation.

9. Support

9.1 A Whistleblower who is our current or former employee can access our Employee Assistance Program. While we may not be able to provide the same level of practical support to non-employee Whistleblowers, we will look at ways to provide support to the extent reasonably possible.

10. Reporting to Regulators

10.1 Nothing in the Policy is intended to restrict a Whistleblower from disclosing Reportable Conduct, providing information to, or communicating with a government agency, law enforcement body or a regulator in accordance with any relevant law or regulation in any jurisdiction in which we conduct business.

11. Breach of Policy

11.1 A breach of this Policy may be regarded as misconduct, which may lead to disciplinary action (including termination of employment or engagement). Any breach of confidentiality of the information provided by a Whistleblower, or of a Whistleblower's identity, and any retaliation against a Whistleblower, will be taken seriously and if appropriate will be separately investigated. An individual who is found to have disclosed the information or to have retaliated (or threatened to retaliate) against a Whistleblower may be subject to

further action (including disciplinary action in the case of employees). An individual may also be exposed to criminal or civil liability for a breach of relevant legislation.

12. Updating the Whistleblowing Policy

12.1 From time to time, and at least annually, we may update this Policy. Any changes to this Policy will be communicated with all employees and any relevant stakeholders and will be approved by resolution of the Board.

13. Reporting to the Board of Directors

13.1 The Board is updated every month on the Policy, and any reports, investigations, and results taken under it. Reports or investigations carrying an undue amount of risk will be reported to the Board outside of the monthly updates. The Board at any time can ask about matters arising or pending under the Policy. The Board is responsible and accountable for oversight of the implementation and effectiveness of the Policy.

Dicker Data – Appendix 1: Channels for Reporting

- via secure postbox located within the Company premises;
- via anonymous email – **whistleblower@dickerdata.com.au**;
- via post to the General Manager, People & Culture and Payroll Manager;
- by speaking with a senior leader at the Company;
- via any additional channels we provide to employees to submit disclosures or anonymous disclosures (e.g., live chat, SMS, voicemail via hotline, fax, etc.)

A Whistleblower can submit a report in person, via phone conversation, in writing, via email or hard copy letter to:

- **Direct Manager;**
- **Senior Manager; or**
- **Company Director.**

Document Management

Revision Date	Nature of Amendments
18 July 2019	Reviewed by the Company Secretary (Erin McMullen)
22 November 2019	Approved by the Board of Dicker Data
13 November 2020	Reviewed by the Company Secretary (Erin McMullen)
20 November 2020	Approved by the Board of Dicker Data
17 December 2021	Approved by the Board of Dicker Data
25 November 2022	Approved by the Board of Dicker Data
22 December 2023	Approved by the Board of Dicker Data