REGULATORY GUIDE 000

Whistleblower policies

August 2019

About this guide

This guide is for entities that must have a whistleblower policy under the Corporations Act—public companies, large proprietary companies and proprietary companies that are trustees of registrable superannuation entities. It gives guidance to help these entities establish, implement and maintain a whistleblower policy that complies with their legal obligations. It also contains our good practice guidance.

This guide will also help entities that are not required to have a whistleblower policy but are required to manage whistleblowing in accordance with the Corporations Act.

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents.

Consultation papers: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

Regulatory guides: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

Information sheets: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

Reports: describe ASIC compliance or relief activity or the results of a research project.

Document history

This draft guide was issued in August 2019 and is based on legislation and regulations as at the date of issue.

Disclaimer

This guide does not constitute legal advice. We encourage you to seek your own professional advice to find out how the *Corporations Act 2001* and other applicable laws apply to you, as it is your responsibility to determine your obligations.

Examples in this guide are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

Contents

A Overview

Key points

The *Corporations Act 2001* (Corporations Act) provides a consolidated whistleblower protection regime for Australia's corporate sector: see Pt 9.4AAA.

The regime requires public companies, large proprietary companies and proprietary companies that are trustees of registrable superannuation entities to have a whistleblower policy and make the policy available to their officers and employees.

We have developed this guidance to help these entities establish, implement and maintain a whistleblower policy that complies with the obligations under the Corporations Act.

We have also included some good practice guidance. This guidance is not mandatory.

Under the regime, ASIC has the power to grant relief from the requirement to have a whistleblower policy in some limited circumstances.

The importance of whistleblower policies

RG 000.1 Transparent whistleblower policies are essential to good risk management and corporate governance. They help uncover misconduct that may not otherwise be detected. Often, such wrongdoing only comes to light because of individuals (acting alone or together) who are prepared to disclose it, sometimes at great personal and financial risk.

RG 000.2 Whistleblower policies help:

(a) provide better protections for individuals who disclose wrongdoing (disclosers);

(b) improve the whistleblowing culture of entities and increase transparency in how entities handle disclosures of wrongdoing;

(c) encourage more disclosures of wrongdoing; and

(d) deter wrongdoing, promote better compliance with the law and promote a more ethical culture, by increasing awareness that there is a higher likelihood that wrongdoing will be reported.

Entities that must have a whistleblower policy

RG 000.3 This guide is for entities that must have a whistleblower policy and make it available to their officers and employees, which are:

(a) public companies;

(b) large proprietary companies; and

(c) proprietary companies that are trustees of registrable superannuation entities (within the meaning of the *Superannuation Industry (Supervision) Act 1993* (SIS Act)).

Note: See s1317AI of the Corporations Act.

Public companies

RG 000.4 All public companies must have a whistleblower policy, including listed companies and public companies that are owned or controlled by the Commonwealth: see s1317AI(1).

Large proprietary companies

RG 000.5 All large proprietary companies must have a whistleblower policy: see s1317AI(2).

RG 000.6 A proprietary company is a large proprietary company for a financial year if it has at least two of the following characteristics:

(a) the consolidated revenue for the financial year of the company and any entities it controls is $50 million or more;

(b) the value of the consolidated gross assets at the end of the financial year of the company and any entities it controls is $25 million or more; and

(c) the company, and any entities it controls, has 100 or more employees at the end of the financial year.

Note: See s45A(3) of the Corporations Act and the Corporations Amendment (Proprietary Company Thresholds) Regulations 2019.

RG 000.7 Once a proprietary company qualifies as a large proprietary company during a financial year, it must have a whistleblower policy and make it available to its officers and employees within six months after the end of that financial year. The company must continue to maintain and make available its whistleblower policy in all subsequent financial years in which it qualifies as a large proprietary company.

Trustees of registrable superannuation entities

RG 000.8 All public companies and proprietary companies that are trustees of registrable superannuation entities (within the meaning of the SIS Act) must have a whistleblower policy: see s1317AI(1) and 1317AI(3).

Other entities that may benefit from this guidance

RG 000.9 The whistleblower protections under the Corporations Act are available to any discloser who qualifies for protection—regardless of whether the entity that is the subject of the disclosure must have a whistleblower policy.

RG 000.10 The information in this guide will help entities that would like to establish mechanisms for managing disclosures on a voluntary basis.

Requirement to have a whistleblower policy

RG 000.11 Section 1317AI(5) requires entities to have a whistleblower policy that covers information about:

(a) the protections available to whistleblowers, including protections under the Corporations Act;

(b) to whom disclosures that qualify for protection under the Corporations Act may be made, and how they may be made;

(c) how the entity will support whistleblowers and protect them from detriment;

(d) how the entity will investigate disclosures that qualify for protection under the Corporations Act;

(e) how the entity will ensure fair treatment of its employees who are mentioned in disclosures that qualify for protection, or its employees who are the subject of disclosures;

(f) how the policy will be made available to officers and employees of the entity; and

(g) any matters prescribed by regulations.

RG 000.12 An entity's whistleblower policy should also include information about the protections provided in the tax whistleblower regime under the *Taxation Administration Act 1953*: see the Revised Explanatory Memorandum to the Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2018 (Whistleblower Protections Bill). For further information about the protections under the tax whistleblower regime, see the Australian Taxation Office's webpage on tax whistleblowers.

Note: Since public companies, large proprietary companies and trustees of registrable superannuation entities are required to have a whistleblower policy under the Corporations Act, such a requirement has not been included in the tax whistleblower provisions.

Complying with the requirements

RG 000.13 To ensure entities have a whistleblower policy that sufficiently meets the objectives set out in RG 000.1–RG 000.2, we expect entities to:

(a) establish a robust and clear whistleblower policy that:

(i) is aligned to the nature, size, scale and complexity of the entity's business;

(ii) is supported by processes and procedures for effectively dealing with disclosures received under the policy; and

(iii) uses a positive tone and language that encourages the disclosure of wrongdoing;

(b) take steps to give effect to their whistleblower policy by ensuring the policy is implemented appropriately and consistently carried out in practice; and

(c) have arrangements in place for periodically reviewing and updating their whistleblower policy to ensure issues are identified and rectified.

Summary of our guidance

RG 000.14 In Section B, we outline:

(a) the matters that must be addressed by an entity's whistleblower policy; and

(b) some good practice guidance on establishing, implementing and maintaining a whistleblower policy, which is not mandatory.

RG 000.15 For a summary of our guidance in Section B, see Table 1.

RG 000.16 In Section C, we outline additional good practice guidance on establishing, implementing and maintaining a whistleblower policy. This guidance is not mandatory.

Table 1: Summary of the matters to be addressed by an entity's whistleblower policy

Component	Matters to be addressed	Further guidance
Purpose of the policy	It is good practice for an entity's whistleblower policy to explain the purpose of the policy. It is also good practice for an entity's whistleblower policy to: • form a part of the entity's risk management system and corporate governance framework; • be one of the mechanisms in the entity's risk management toolkit for identifying wrongdoing; and • be available to all employees as part of their employment information.	RG 000.27–RG 000.30
Who the policy applies to (see s1317AI(5)(a))	An entity's whistleblower policy should identify the different types of disclosers within and outside the entity who can make a disclosure that qualifies for protection (i.e. 'eligible whistleblowers'). The policy should set out the criteria for a discloser to qualify for protection as a whistleblower under the Corporations Act.	RG 000.31–RG 000.36
Matters the policy applies to (see s1317AI(5)(b))	An entity's whistleblower policy should identify the types of wrongdoing that can be reported (i.e. 'disclosable matters'). In addition, it should outline the types of matters that are not covered by the policy (e.g. personal work-related grievances).	RG 000.37–RG 000.55
Who can provide advice on or receive a disclosure (see s1317AI(5)(b))	An entity's whistleblower policy must identify the types of people within and outside the entity who can provide advice on or receive a disclosure that qualifies for protection—that is: • 'eligible recipients'; • legal practitioners; • regulatory bodies and other external parties; • journalists; and • members of Commonwealth, state or territory parliaments (parliamentarians).	RG 000.56–RG 000.71
Roles and responsibilities	It is good practice for an entity's whistleblower policy to outline the key roles and responsibilities under its whistleblower policy (e.g. a role responsible for protecting or safeguarding disclosers and ensuring the integrity of the reporting mechanism).	RG 000.72–RG 000.83
How to make a disclosure (see s1317AI(5)(b))	An entity's whistleblower policy must include information about how to make a disclosure. The policy should outline the different options available for making a disclosure. The options should allow for disclosures to be made anonymously and/or confidentially, securely and outside of business hours. It should also include information about how to access each option, along with the relevant instructions. The policy should advise that disclosures can be made anonymously and still be protected under the Corporations Act.	RG 000.84–RG 000.96

Component	Matters to be addressed	Further guidance
Legal protections for disclosers (see s1317AI(5)(a))	An entity's whistleblower policy must include information about the protections available to disclosers who qualify for protection as a whistleblower, including the protections under the Corporations Act. These protections are: • identity protection (confidentiality); • protection from detrimental acts or omissions; • compensation and remedies; and • civil, criminal and administrative liability protection. An entity's policy should outline the measures the entity has in place for protecting the confidentiality of a discloser's identity.	RG 000.97–RG 000.116
Support and practical protection for disclosers (see s1317AI(5)(c))	An entity's whistleblower policy must outline the entity's measures for supporting disclosers and protecting disclosers from detriment in practice. An entity should assess the risk of detriment to the discloser or another person in relation to a disclosure, as soon as it receives a disclosure.	RG 000.117–RG 000.129
Handling and investigating a disclosure (see s1317AI(5)(d))	An entity's whistleblower policy must include information about how it will investigate disclosures that qualify for protection. The policy should outline the steps the entity will take after it receives a disclosure, including how it: • investigates a disclosure; • keeps a discloser informed; and • documents, reports internally and communicates to the discloser the investigation findings.	RG 000.130–RG 000.149
Ensuring fair treatment of individuals mentioned in a disclosure (see s1317AI(5)(e))	An entity's whistleblower policy must include information about how the entity will ensure the fair treatment of employees who are mentioned in a disclosure that qualifies for protection, including those who are the subject of a disclosure.	RG 000.150–RG 000.152
Ensuring the policy is easily accessible (see s1317AI(5)(f)	An entity's whistleblower policy must cover how the policy will be made available to the entity's officers and employees. It should outline the entity's measures for ensuring its policy is widely disseminated to and easily accessible by disclosers within and outside the entity (e.g. through upfront and ongoing education and training for its employees).	RG 000.153–RG 000.164
Monitoring and reporting on the effectiveness of the policy	As a matter of good practice, an entity's whistleblower policy should be supported by arrangements for monitoring the effectiveness of its policy, processes and procedures.	RG 000.166–RG 000.177
Reviewing and updating the policy	As a matter of good practice, an entity's whistleblower policy, processes and procedures should be reviewed and updated on a periodic basis.	RG 000.178–RG 000.182

Our regulatory powers

Power to grant relief by legislative instrument

RG 000.17 Under the regime, ASIC has the power to make an order by legislative instrument to relieve a specified class of entities from the requirement to have a whistleblower policy: see s1317AJ.

RG 000.18 We can only use this power in some limited circumstances—specifically, if the benefits of the whistleblower policy requirement, in encouraging good corporate culture and governance, are outweighed by reduced flexibility and unnecessarily high compliance costs (as outlined in the Revised Explanatory Memorandum to the Whistleblower Protections Bill). For further information, see Regulatory Guide 51 *Applications for relief* (RG 51).

Penalty for non-compliance

RG 000.19 Failure to comply with the requirement to have and make available a whistleblower policy is an offence of strict liability with a penalty of 60 penalty units (currently $12,600), enforceable by ASIC: see s1317AI(4) and 1311(1).

B Matters to be addressed by an entity's whistleblower policy

Key points

This section provides guidance to help entities establish, implement and maintain a whistleblower policy that complies with their legal obligations. It also includes some good practice guidance, which is not mandatory.

The matters to be addressed by an entity's whistleblower policy are:

- purpose of the policy (see RG 000.27–RG 000.30);
- who the policy applies to (see RG 000.31–RG 000.36);
- matters the policy applies to (see RG 000.37–RG 000.55);
- who can provide advice on or receive a disclosure (see RG 000.56–RG 000.71);
- roles and responsibilities (see RG 000.72–RG 000.83);
- how to make a disclosure (see RG 000.84–RG 000.96);
- legal protections for disclosers (see RG 000.97–RG 000.116);
- support and practical protection for disclosers (see RG 000.117–RG 000.129);
- handling and investigating a disclosure (see RG 000.130–RG 000.149);
- ensuring fair treatment of individuals mentioned in a disclosure (see RG 000.150–RG 000.152);
- ensuring the policy is easily accessible (see RG 000.153–RG 000.165);
- monitoring and reporting the effectiveness of the policy (see RG 000.166–RG 000.177); and
- reviewing and updating the policy (see RG 000.178–RG 000.182).

Approach to our guidance

RG 000.20 In this section, we outline:

(a) the matters that must be addressed by an entity's whistleblower policy; and

(b) some good practice guidance on establishing, implementing and maintaining a whistleblower policy, which is not mandatory.

RG 000.21 The matters we have included in this section reflect all stages of the whistleblowing process:

(a) providing advice to individuals who are considering making a disclosure;

(b) receiving a disclosure;

(c) assessing how a discloser should be supported and protected;

(d) assessing whether a disclosure should be investigated;

(e) undertaking an investigation;

(f) supporting and protecting a discloser during and after the investigation;

(g) communicating with a discloser, including about the outcome of an investigation; and

(h) ensuring oversight and monitoring by the entity's board.

RG 000.22 Our guidance also reflects that, if a discloser seeks compensation and other remedies through the courts because they have suffered detriment, including because a discloser's employer failed to prevent detriment from occurring, the court may take into account the extent to which the employer gave effect to their whistleblower policy (if the entity has a policy in place): see s1317AE(3)(b).

RG 000.23 In addition, the guidance is consistent with research on whistleblowing management. Research indicates that an entity's whistleblower policy plays a critical role in the overall management of whistleblowing by the entity; however:

(a) having a formal whistleblower policy is not enough; and

(b) even if the objectives and approach of a whistleblower policy are correct, the policy will not be meaningful and effective unless it is implemented consistently and applied throughout the entity in practice.

Note: See AJ Brown and SA Lawrence, *Strength of organisational whistleblowing processes—Analysis from Australia & New Zealand: Further results: Whistling While They Work 2* (PDF 757 KB), report, Griffith University, July 2017. ASIC is a member of the Whistling While They Work 2 research project.

Structuring, drafting and presenting a whistleblower policy

RG 000.24 This section is also intended to provide entities with a potential structure from which to develop their own whistleblower policy.

RG 000.25 The requirement to have a whistleblower policy applies to entities of varying sizes that operate in different sectors. We recognise that there is no one-size-fits-all whistleblower policy. We expect an entity to analyse how best to structure, draft and present its policy. We also expect an entity to consider other standards and guidelines to ensure its whistleblower policy, processes and procedures incorporate current developments and best practice in preventing and responding to misconduct.

RG 000.26 Regardless of how an entity presents its whistleblower policy, we expect the content to cover the information required under the Corporations Act: see s1317AI(5).

Purpose of the policy

Good practice guidance

RG 000.27 As a matter of good practice, an entity's whistleblower policy should explain the purpose of the policy—for example, to:

(a) ensure individuals who disclose wrongdoing can do so safely, securely and with confidence that they will be protected and supported;

(b) ensure disclosures are dealt with appropriately and on a timely basis;

(c) provide transparency around the entity's framework for receiving, handling and investigating disclosures;

(d) encourage more disclosures of wrongdoing; and

(e) help deter wrongdoing.

RG 000.28 The policy could also include the following, as the rationale for the policy:

(a) to support the entity's values, code of conduct and/or ethics policy;

(b) to support the entity's long-term sustainability and reputation;

(c) to meet the entity's legal and regulatory obligations; and

(d) to align with the ASX Corporate Governance Principles and Recommendations (which applies to listed companies) and relevant standards.

RG 000.29 It is good practice for an entity's policy to include a statement about the importance of disclosures to the entity's risk management and corporate governance framework. The policy could explain that the entity's whistleblower policy is a practical tool for helping the entity to identify wrongdoing that may not be uncovered unless there is a safe and secure means for disclosing wrongdoing. An entity's policy could also include specific statements encouraging the entity's employees (and non-employees) who are aware of possible wrongdoing to have the confidence to speak up.

RG 000.30 It is also good practice for an entity's policy to be included in the entity's employment information.

Who the policy applies to

RG 000.31 An entity's whistleblower policy should identify the different types of disclosers within and outside the entity who can make a disclosure that qualifies for protection under the Corporations Act (i.e. 'eligible whistleblowers'): see s1317AI(5)(a).

RG 000.32 If an entity is a body corporate, an eligible whistleblower is an individual who is, or has been, any of the following in relation to the entity:

(a) an officer or employee;

(b) a supplier of services or goods to the entity (whether paid or unpaid), including their employees;

(c) an associate of the entity; and

(d) a relative, dependant or spouse of an individual in RG 000.32(a)–RG 000.32(c).

RG 000.33 If an entity is a superannuation entity, an eligible whistleblower is an individual who is, or has been, any of the following in relation to the entity:

(a) a trustee, custodian or investment manager, including their employees;

(b) a supplier of services or goods to the trustee, custodian or investment manager (whether paid or unpaid), including their employees;

(c) an officer, employee or supplier of services or goods (whether paid or unpaid), including their employees, of a body corporate that is a trustee, custodian or investment manager of a superannuation entity; or

(d) a relative, dependant or spouse of an individual in RG 000.33(a)–RG 000.33(c).

Note: See s1317AAA of the Corporations Act.

RG 000.34 The policy should set out that a discloser qualifies for protection as a whistleblower under the Corporations Act if they are an 'eligible whistleblower' in relation to the entity and:

(a) they have made a disclosure of information relating to a 'disclosable matter' directly to an 'eligible recipient' or to ASIC, the Australian Prudential Regulation Authority (APRA) or another Commonwealth body prescribed by regulation;

(b) they have made a disclosure to a legal practitioner for the purposes of obtaining legal advice or legal representation about the operation of the whistleblower provisions in the Corporations Act; or

(c) they have made an 'emergency disclosure' or 'public interest disclosure'.

Note: See s1317AA, s1317AAA, s1317AAC and 1317AAD of the Corporations Act.

Good practice guidance

RG 000.35 It is good practice to include a list of the types of disclosers who are covered by the policy, based on the entity's business operations, practices and organisational structure and set up. Some examples include:

(a) current and former employees, including employees who are permanent, part time, fixed term or temporary, interns, secondees, managers, and directors; and

(b) current and former contractors, consultants, service providers, suppliers and business partners.

RG 000.36 Where relevant, a whistleblower policy should outline the businesses, divisions and offices that are covered by the policy. Due to varying whistleblowing legislation across jurisdictions, multinational entities should consider whether it would be more appropriate to establish, implement and maintain a standalone whistleblower policy for their Australian operations.

Matters the policy applies to

RG 000.37 An entity's whistleblower policy should identify the types of wrongdoing that can be reported under the policy: see s1317AI(5)(b). In addition, it should outline the types of matters that are not covered by the policy.

Disclosable matters

RG 000.38 An entity's policy should cover the types of disclosures that qualify for protection under the Corporations Act (i.e. 'disclosable matters'): see s1317AA.

RG 000.39 Disclosable matters involve information that the discloser has reasonable grounds to suspect concerns misconduct, or an improper state of affairs or circumstances, in relation to:

(a) an entity; or

(b) if the entity is a body corporate, a related body corporate of the entity.

Note: See s1317AA(4). The term 'misconduct' is defined in s9 of the Corporations Act to include 'fraud, negligence, default, breach of trust and breach of duty'. The phrase 'improper state of affairs or circumstances' is not defined and is intentionally broad.

RG 000.40 Disclosable matters also involve information about an entity in RG 000.39, if the discloser has reasonable grounds to suspect that the information indicates those entities (including their employees or officers) have engaged in conduct that:

(a) constitutes an offence against, or a contravention of, a provision of any of the following:

(i) the Corporations Act;

(ii) the *Australian Securities and Investments Commission Act 2001*;

(iii) the *Banking Act 1959*;

(iv) the *Financial Sector (Collection of Data) Act 2001*;

(v) the *Insurance Act 1973*;

(vi) the *Life Insurance Act 1995*;

(vii) the *National Consumer Credit Protection Act 2009*;

(viii) the SIS Act;

(ix) an instrument made under an Act referred to in RG 000.40(a)(i)–RG 000.40(a)(viii);

(b) constitutes an offence against any other law of the Commonwealth that is punishable by imprisonment for a period of 12 months or more;

(c) represents a danger to the public or the financial system; or

(d) is prescribed by regulation.

Note: See s1317AA(5) of the Corporations Act. The more specific categories of conduct set out in s1317AA(5) do not limit the range of misconduct covered by s1317AA(4), or vice versa. Rather, they make clear that certain forms of conduct qualify for protection.

RG 000.41 An entity's policy should explain that disclosable matters include conduct that may not involve a contravention of a particular law. For example, 'misconduct or an improper state of affairs or circumstances' may not involve unlawful conduct in relation to the entity or a related body corporate of the entity but may indicate a systemic issue that the relevant regulator should know about to properly perform its functions. It may also relate to dishonest or unethical behaviour and practices, conduct that may cause harm, or conduct prohibited by the entity's standards or code(s) of conduct.

RG 000.42 An entity's policy should also explain that 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.

RG 000.43 In addition, the policy should explain that a discloser can still qualify for protection even if their disclosure turns out to be incorrect.

RG 000.44 The term 'reasonable grounds to suspect' is based on the objective reasonableness of the reasons for the discloser's suspicion. It ensures that a discloser's motive for making a disclosure, or their personal opinion of the person(s) involved, does not prevent them from qualifying for protection. In practice, a mere allegation with no supporting information is not likely to be considered as having 'reasonable grounds to suspect'. However, a discloser does not need to prove their allegations.

Good practice guidance

RG 000.45 It is good practice for a whistleblower policy to include examples of disclosures that relate specifically to an entity's business operations and practices. Some examples include:

(a) illegal conduct, such as theft, dealing in, or use of illicit drugs, violence or threatened violence, and criminal damage against property;

(b) fraud, money laundering or misappropriation of funds;

(c) offering or accepting a bribe;

(d) financial irregularities;

(e) failure to comply with, or breach of, legal or regulatory requirements; and

(f) 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.

RG 000.46 An entity's whistleblower policy could include a statement discouraging deliberate false reporting. However, an entity needs to ensure that they do not unintentionally deter staff from making disclosures (e.g. disclosers who have some information leading to a suspicion, but not all the details).

RG 000.47 Deliberate false reports involve a discloser reporting information they know to be untrue. It does not include situations where a discloser reasonably suspects misconduct, but their suspicions are later determined to be unfounded.

RG 000.48 An entity's policy could highlight that individuals who deliberately submit false reports will not able to access the whistleblower protections under the Corporations Act. It could also include an explanation about the potential consequences of deliberate false reporting to the entity's reputation and the reputation of individuals who are mentioned in false reports.

Types of disclosures not covered by the policy

RG 000.49 An entity's policy should clarify that disclosures that are not about disclosable matters are not covered by the policy because they do not qualify for protection under the Corporations Act. It should, however, note that such disclosures may be protected under other legislation, such as the *Fair Work Act 2009* (Fair Work Act).

Personal work-related grievances

RG 000.50 Disclosures that relate solely to personal work-related grievances, and that do not relate to detriment or threat of detriment to the discloser, do not

qualify for protection under the Corporations Act: see s1317AADA(1) and s1317AC.

RG 000.51 Personal work-related grievances are those that relate to the discloser's current or former employment and have, or tend to have, implications for the discloser personally, but do not:

(a) have any other significant implications for the entity (or another entity); or

(b) relate to any conduct, or alleged conduct, about a disclosable matter (as set out in RG 000.39–RG 000.40).

Note: See s1317AADA(2). Workplace grievances remain the jurisdiction of the Fair Work Act.

RG 000.52 Examples of grievances that may be personal work-related grievances include:

(a) an interpersonal conflict between the discloser and another employee; and

(b) decisions that do not involve a breach of workplace laws:

(i) about the engagement, transfer or promotion of the discloser;

(ii) about the terms and conditions of engagement of the discloser; or

(iii) to suspend or terminate the engagement of the discloser, or otherwise to discipline the discloser.

RG 000.53 An entity's policy should define 'personal work-related grievance' and include some examples. The policy should explain when a disclosure about, or including, a personal work-related grievance still qualifies for protection. For example, if:

(a) a personal work-related grievance includes information about misconduct, or information about misconduct includes or is accompanied by a personal work-related grievance (mixed report);

(b) the entity 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;

(c) the discloser suffers from or is threatened with detriment for making a disclosure (see RG 000.50 and RG 000.108–RG 000.112); or

(d) the discloser seeks legal advice or legal representation about the operation of the whistleblower protections under the Corporations Act (see RG 000.64).

RG 000.54 It is important for an entity to focus on the substance of the disclosure, rather than what they believe to be the discloser's motive for reporting. It is also

important for an entity not to assume that disclosures about conduct or behaviour that appear to have had a personal impact on a discloser are somehow less serious. The discloser's experience may indicate a larger or systemic issue. For example, bullying or harassment experienced by the discloser may be representative of a more general culture of bullying or harassment in the entity or may indicate an environment where other misconduct is occurring.

Good practice guidance

RG 000.55 It is good practice for an entity's whistleblower policy to provide information about how its employees can internally raise personal work-related grievances and other types of issues or concerns that are not covered by the policy. It could also encourage employees to seek legal advice about their rights and protections under employment or contract law, and how to resolve their personal work-related grievance.

Who can provide advice on or receive a disclosure

RG 000.56 An entity's whistleblower policy must identify the types of people within and outside the entity who can provide advice on or receive a disclosure that qualifies for protection: see s1317AI(5)(b).

Eligible recipients in relation to the entity

RG 000.57 An entity's policy should explain the role of eligible recipients—that is, to receive disclosures that qualify for protection. The policy should highlight that a discloser needs to make a disclosure directly to one of the entity's eligible recipients to be able to qualify for protection as a whistleblower under the Corporations Act. It should also highlight that a discloser qualifies for protection from the time they make their disclosure, regardless of whether the discloser or recipient recognises that the disclosure qualifies for protection.

RG 000.58 If an entity is a body corporate, an eligible recipient includes:

(a) an officer or senior manager of the entity or related body corporate;

(b) the internal or external auditor (including a member of an audit team conducting an audit) or actuary of the entity or related body corporate; and

(c) a person authorised by the entity to receive disclosures that may qualify for protection.

Note: See 1317AAC(1) of the Corporations Act.

RG 000.59 If an entity is a superannuation entity, an eligible recipient includes:

(a) an officer of the entity;

(b) the entity's internal or external auditor (including a member of an audit team conducting an audit), or actuary;

(c) an individual who is the trustee of the entity;

(d) a director of a body corporate that is the trustee of the entity; and

(e) a person authorised by the trustee(s) to receive disclosures that may qualify for protection.

Note: See s1317AAC(2) of the Corporations Act.

RG 000.60 Generally, an 'officer' includes a director or company secretary of an entity.

RG 000.61 A 'senior manager' is generally a senior executive within an entity, other than a director or company secretary, who:

(a) makes or participates in making decisions that affect the whole, or a substantial part, of the business of the entity; or

(b) has the capacity to significantly affect the entity's financial standing.

Note: See s9 of the Corporations Act.

Good practice guidance

RG 000.62 It is good practice for an entity's policy to encourage its employees and external disclosers to make a disclosure to the entity in the first instance. However, the entity needs to ensure that its policies, processes and procedures make it safe for disclosers to do so.

RG 000.63 The policy could include a statement that the entity would like to identify and address wrongdoing as early as possible. It could also acknowledge that a discloser can make a disclosure directly to regulatory bodies, or other external parties, about a disclosable matter and qualify for protection under the Corporations Act without making a prior disclosure to the entity: see RG 000.65. In addition, it could highlight that the entity's approach is intended to help build confidence and trust in its whistleblower policy, processes and procedures.

Legal practitioners

RG 000.64 An entity's policy should explain that 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 in the event the legal practitioner concludes that a disclosure does not relate to a 'disclosable matter'): see s1317AA(3).

Regulatory bodies and other external parties

RG 000.65 An entity's policy should explain that 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: see s1317AA(1).

Good practice guidance

RG 000.66 It is good practice for an entity's policy to provide advice about how an employee can make a disclosure outside the entity and qualify for protection, if an employee believes it is necessary to contact regulatory bodies or other external parties.

RG 000.67 An entity's policy could include links to whistleblowing information provided by ASIC or APRA, such as ASIC Information Sheet 239 *How ASIC handles whistleblower reports* (INFO 239).

Public interest disclosures and emergency disclosures

RG 000.68 An entity's policy should explain that disclosures can be made to a journalist or parliamentarian under certain circumstances and qualify for protection: see s1317AAD.

RG 000.69 A 'public interest disclosure' is the disclosure of information to a journalist or a parliamentarian, where:

(a) at least 90 days have passed since the discloser made the disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation;

(b) the discloser does not have reasonable grounds to believe that action is being, or has been taken, in relation to their disclosure;

(c) the discloser has reasonable grounds to believe that making a further disclosure of the information is in the public interest; and

(d) before making the public interest disclosure, the discloser has given written notice to the body in RG 000.69(a) (i.e. the body to which the previous disclosure was made) that:

(i) includes sufficient information to identify the previous disclosure; and

(ii) states that the discloser intends to make a public interest disclosure.

Note: See s1317AAD(1) of the Corporations Act.

RG 000.70 An 'emergency disclosure' is the disclosure of information to a journalist or parliamentarian, where:

(a) the discloser has previously made a disclosure of the information to ASIC, APRA or another Commonwealth body prescribed by regulation;

(b) the discloser has reasonable grounds to believe that the information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment;

(c) before making the emergency disclosure, the discloser has given written notice to the body in RG 000.70(a) (i.e. the body to which the previous disclosure was made) that:

(i) includes sufficient information to identify the previous disclosure; and

(ii) states that the discloser intends to make an emergency disclosure; and

(d) the extent of the information disclosed in the emergency disclosure is no greater than is necessary to inform the journalist or parliamentarian of the substantial and imminent danger.

Note: See s1317AAD(2) of the Corporations Act.

Good practice guidance

RG 000.71 It is good practice for an entity's whistleblower policy to include a statement suggesting that a discloser should contact the entity's whistleblower protection officer or an independent legal adviser to ensure a discloser understands the criteria for making a public interest or emergency disclosure that qualifies for protection.

Roles and responsibilities

RG 000.72 An entity's board is ultimately responsible for ensuring that the entity has an appropriate risk management framework to identify and manage risks on an ongoing basis.

Good practice guidance

RG 000.73 As a matter of good practice, an entity should outline the key roles and responsibilities under its whistleblower policy. For example:

(a) a contact point where employees can seek accurate and confidential advice or information about the following, without making a disclosure:

(i) how the entity's whistleblower policy works;

(ii) what the policy covers; and

(iii) how a disclosure might be handled.

(b) specific roles for receiving disclosures directly from disclosers (i.e. internal reporting points), which are staff members who are 'eligible recipients';

(c) an independent whistleblowing service provider that the entity has authorised to directly receive disclosures;

(d) a role responsible for protecting or safeguarding disclosers and ensuring the integrity of the reporting mechanism (i.e. a 'whistleblower protection officer' or equivalent);

(e) a role responsible for investigating disclosures (i.e. a 'whistleblower investigation officer' or equivalent);

(f) legal counsel and human resources staff who may assist the entity with specific investigations;

(g) other types of third-party service providers—such as investigation firms and financial, legal and other advisers—that the entity may engage to assist with investigating disclosures;

(h) an officer responsible for periodically reviewing and updating the whistleblower policy, processes and procedures, and for implementing and overseeing any changes;

(i) the owner of the whistleblower policy (e.g. the board of directors—either directly or through the audit or risk committee—or an independent director), who is also responsible for oversight and monitoring of the policy; and

(j) a board committee responsible for approving updates to the policy, processes and procedures (e.g. the audit or risk committee).

Note: See guidance on an entity's legal obligations to protect the confidentiality of a discloser's identity at RG 000.100–RG 000.107.

Whistleblower protection and investigation officers

RG 000.74 In practice, the roles of internal reporting point and whistleblower protection officer could be held by the same staff member.

RG 000.75 It is good practice for an entity's whistleblower policy to nominate eligible recipients who are outside the chain of command as the whistleblower protection officer and whistleblower investigation officer. It is also good practice for these roles to be allocated to different eligible recipients, and for the officers to act independently of each other.

RG 000.76 The whistleblower protection officer should report directly to the entity's board or audit or risk committee. They should be given direct access to independent advisers. The whistleblower investigation officer should report directly to a senior executive or officer with responsibility for legal, compliance or risk matters.

RG 000.77 Larger entities could create new roles for the whistleblower protection officer and whistleblower investigation officer. Alternatively, the

responsibilities can be integrated into existing roles that are involved in performing integrity and compliance functions.

RG 000.78 Larger entities or geographically dispersed entities could appoint a number of whistleblower protection officers who report to an individual who is appointed as the coordinator of the entity's whistleblower policy. In addition, they could appoint a number of whistleblower investigation officers.

RG 000.79 It is good practice for an entity to ensure that any individual in the entity (e.g. an 'eligible recipient' or the discloser's supervisor or manager) who receives a disclosure notifies the entity's whistleblower protection officer, subject to the discloser's consent, to ensure that the entity's mechanisms for protecting and safeguarding disclosers can commence as soon as possible.

Independent whistleblowing service providers

RG 000.80 Some entities could consider authorising an independent whistleblowing service provider as an 'eligible recipient' for directly receiving some of their disclosures (e.g. a telephone hotline or online platform). This may help provide greater confidence to the entity's employees. It may also provide better access for the entity's external disclosers.

RG 000.81 If an entity authorises an independent whistleblowing service provider, it is good practice for the entity's policy to explain the rationale. For example, to:

(a) act as an intermediary between the entity and disclosers;

(b) enable disclosures to be made:

  (i) anonymously;

  (ii) confidentially; and

  (iii) outside of business hours;

(c) enable disclosers to retain their anonymity while allowing the entity to obtain additional information; and

(d) enable disclosers to receive updates on the status of their disclosure while retaining anonymity.

RG 000.82 In the case of smaller entities, particularly those with a limited number of employees, it might not be possible to allocate all the responsibilities for providing advice on, receiving, handling and investigating disclosures to its staff members. It is good practice for these entities to consider authorising an independent whistleblowing service provider as an eligible recipient for receiving disclosures (i.e. by its employees and non-employees) to help avoid any potential conflicts of interest and to provide better protections to disclosers. It is also good practice for these entities to consider engaging an independent investigation firm.

Responsibility for outsourced functions

RG 000.83 It is important to note that the entity remains responsible for meeting its legal obligations for outsourced functions (e.g. obligations relating to confidentiality). The entity should ensure it undertakes appropriate due diligence before engaging an independent whistleblowing service provider and other third-party service providers. It should also ensure that it has mechanisms for monitoring the services outsourced.

How to make a disclosure

RG 000.84 An entity's whistleblower policy must include information about how to make a disclosure: see s1317AI(5)(b).

RG 000.85 An entity's policy should outline the different options for making a disclosure. The options should allow for disclosures to be made anonymously and/or confidentially, securely and outside of business hours.

RG 000.86 It should specify the names of the entity's internal reporting points and the whistleblower protection officer. Larger entities, particularly geographically dispersed entities, should include information about the internal reporting points and whistleblower protection officer for each site.

RG 000.87 In addition, it should emphasise that a discloser can make a disclosure directly to any of the entity's 'eligible recipients', not just its internal reporting points, and qualify for protection.

RG 000.88 The policy should include information about how to access each option, along with the relevant instructions. For example, the policy can include:

(a) information on how to contact the entity's internal reporting points in person or through post or email;

(b) the telephone number for the entity's internal whistleblower hotline or the entity-authorised external hotline; and

(c) a link to the entity-authorised external whistleblower platform.

RG 000.89 Providing a range of internal and external disclosure options will ensure employees who are not comfortable making a disclosure internally, or feel it is inappropriate to do so, can still make a disclosure to the entity. It also sends a positive message that the entity values all disclosures and that employees should not be deterred by barriers such as threat of detriment.

RG 000.90 The availability of an external reporting option will better enable the entity's non-employees (e.g. former employees and current and former suppliers) to make a disclosure to the entity.

Anonymous disclosures

RG 000.91 An entity's policy should include a statement advising that disclosures can be made anonymously and still be protected under the Corporations Act: see s1317AAE.

RG 000.92 The policy should explain that a discloser can choose to remain anonymous while making a disclosure, over the course of the investigation and after the investigation is finalised. It should also explain that a discloser can refuse to answer questions that they feel could reveal their identity during follow-up conversations.

RG 000.93 The policy should also explain that a discloser may choose to adopt a pseudonym for the purposes of their disclosure, and not use their true name. This may be appropriate in circumstances where the discloser's identity is known to their supervisor, the internal reporting point or whistleblower protection officer, but the discloser prefers not to disclose their identity to others.

RG 000.94 If a disclosure comes from an email address from which the person's identity cannot be determined, and the discloser does not identify themselves in the email, it should be treated as an anonymous disclosure.

Good practice guidance

RG 000.95 It is good practice for the policy to suggest that a discloser who wishes to remain anonymous should maintain ongoing two-way communication with the entity, so the entity can ask follow-up questions or provide feedback.

RG 000.96 Due to advances in technology, services that enable entities to communicate with anonymous disclosers, while ensuring the discloser's anonymity, are now available—for example anonymous telephone hotlines and anonymised email addresses (anonymous channels).

Legal protections for disclosers

RG 000.97 An entity's whistleblower policy must include information about the protections under the Corporations Act that are available to disclosers who qualify for protection as a whistleblower: see s1317AI(5)(a).

RG 000.98 The policy should cover the following protections:

(a) identity protection (confidentiality) (see RG 000.100–RG 000.107);

(b) protection from detrimental acts or omissions (see RG 000.108–RG 000.112);

(c) compensation and other remedies (see RG 000.113–RG 000.114); and

(d) civil, criminal and administrative liability protection (see RG 000.115–RG 000.116).

RG 000.99 The policy should explain that the protections apply not only to internal disclosures, but to disclosures to legal practitioners, regulatory and other external bodies, and public interest and emergency disclosures that are made in accordance with the Corporations Act.

Identity protection (confidentiality)

RG 000.100 An entity's whistleblower policy should explain the entity's legal obligations to protect the confidentiality of a discloser's identity.

RG 000.101 A person cannot disclose the identity of a discloser or information that is likely to lead to the identification of the discloser (which they have obtained directly or indirectly because the discloser made a disclosure that qualifies for protection).

RG 000.102 The exception to RG 000.101 is if a person discloses the identity of the discloser:

(a) to ASIC, APRA, or a member of the Australian Federal Police (within the meaning of the *Australian Federal Police Act 1979*);

(b) to a legal practitioner (for the purposes of obtaining legal advice or legal representation about the whistleblower provisions in the Corporations Act);

(c) to a person or body prescribed by regulations; or

(d) with the consent of the discloser.

RG 000.103 A person can disclose the information contained in a disclosure without the discloser's consent if:

(a) the information does not include the discloser's identity;

(b) the entity has taken all reasonable steps to reduce the risk that the discloser will be identified from the information; and

(c) it is reasonably necessary for investigating the issues raised in the disclosure.

RG 000.104 ASIC, APRA or the Australian Federal Police can disclose the identity of the discloser, or information that is likely to lead to the identification of the discloser, to a Commonwealth, state or territory authority to help the authority in the performance of its functions or duties.

Note: See s1317AAE of the Corporations Act.

RG 000.105 An entity's policy should explain that it is illegal for a person to identify a discloser, or disclose information that is likely to lead to the identification of the discloser, outside the exceptions in RG 000.102–RG 000.104.

RG 000.106 An entity's policy should include information about how a discloser can lodge a complaint with the entity about a breach of confidentiality. It should

also explain that a discloser may lodge a complaint with a regulator, such as ASIC or APRA, for investigation.

RG 000.107 An entity's policy should outline the measures the entity has in place for ensuring confidentiality. An entity should establish secure record-keeping and information sharing procedures. It should ensure that:

(a) all paper and electronic documents and other materials relating to disclosures are stored securely;

(b) all information relating to a disclosure can only be accessed by those directly involved in managing and investigating the disclosure;

(c) only a restricted number of people who are directly involved in handling and investigating a disclosure are made aware of a discloser's identity or information that is likely to lead to the identification of the discloser;

(d) communications and documents relating to the investigation of a disclosure are not sent to an email address or to a printer that can be accessed by other staff; and

(e) each person who is involved in handling and investigating a disclosure is reminded that they should keep the identity of the discloser and the disclosure confidential and that an unauthorised disclosure of a discloser's identity may be a criminal offence.

Protection from detrimental acts or omissions

RG 000.108 An entity's whistleblower policy should explain the legal protections for protecting a discloser, or any other person, from detriment in relation to a disclosure.

RG 000.109 A person cannot engage in conduct that causes detriment to a discloser (or another person), in relation to a disclosure, if:

(a) the person believes or suspects that the discloser (or another person) made, may have made, proposes to make or could make a disclosure that qualifies for protection; and

(b) the belief or suspicion is the reason, or part of the reason, for the conduct.

RG 000.110 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.

Note: See s1317AC of the Corporations Act.

RG 000.111 The policy should provide examples of detrimental conduct which are prohibited under the law, without deterring employees from making disclosures. Examples of detrimental conduct include:

(a) dismissal of an employee;

(b) injury of an employee in his or her employment;

(c) alteration of an employee's position or duties to his or her disadvantage;

(d) discrimination between an employee and other employees of the same employer;

(e) harassment or intimidation of a person;

(f) harm or injury to a person, including psychological harm;

(g) damage to a person's property;

(h) damage to a person's reputation;

(i) damage to a person's business or financial position; or

(j) any other damage to a person.

Note: See s1317ADA of the Corporations Act.

RG 000.112 The policy should also provide examples of actions that are not detrimental conduct. In practice, administrative action that is reasonable to protect a discloser from detriment (e.g. when the disclosure relates to wrongdoing in the discloser's immediate work area) will not be considered as detrimental conduct. Protecting a discloser from detriment also does not prevent the entity from managing a discloser's unsatisfactory work performance, if the action is in line with the entity's performance management framework. It is important for an entity to ensure that a discloser understands the reason for the entity's administrative or management action.

Compensation and other remedies

RG 000.113 An entity's whistleblower policy should outline that a discloser (or any other employee or person) can seek compensation and other remedies through the courts if:

(a) they suffer loss, damage or injury because of a disclosure; and

(b) the entity failed to prevent a person from causing the detriment.

Note: See s1317AD of the Corporations Act.

RG 000.114 The policy should include a statement encouraging disclosers to seek independent legal advice.

Civil, criminal and administrative liability protection

RG 000.115 An entity's whistleblower policy should explain that a discloser is protected from any of the following in relation to their disclosure:

(a) civil liability (e.g. any legal action against the discloser for breach of an employment contract, duty of confidentiality or another contractual obligation);

(b) 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

(c) administrative liability (e.g. disciplinary action for making the disclosure).

RG 000.116 It should also explain that the protections do not grant immunity for any misconduct a discloser has engaged in that is revealed in their disclosure.

Note: see s1317AB(1) of the Corporations Act.

Support and practical protection for disclosers

RG 000.117 An entity's policy must include information about how it will support disclosers and protect disclosers from detriment: see s1317AI(5)(c).

Identity protection (confidentiality)

RG 000.118 An entity's whistleblower protection officer should provide assurance to a discloser that the entity is committed to protecting the confidentiality of their identity.

RG 000.119 The whistleblower protection officer should explain the procedures the entity has in place for ensuring confidentiality. The whistleblower protection officer should also explain that people may be able to guess the discloser's identity if:

(a) the discloser has previously mentioned to other people that they are considering making a disclosure;

(b) the discloser is one of a very small number of people with access to the information; or

(c) the disclosure relates to information that a discloser has previously been told privately and in confidence.

Protection from detrimental acts or omissions

RG 000.120 An entity's policy should explain how the entity will, in practice, protect disclosers from detriment. For example, it should explain:

(a) how whistleblower protection officer(s) will protect the welfare of disclosers;

(b) processes for assessing the risk of detriment against a discloser and other persons (e.g. other staff who might be suspected to have made a disclosure) as soon as possible after receiving a disclosure;

(c) support services (including counselling or other professional or legal services) that are available to disclosers;

(d) strategies to help a discloser minimise and manage stress, time or performance impacts, or other challenges resulting from the disclosure or its investigation;

(e) the specific actions the entity will take to protect a discloser from risk of detriment (e.g. the entity could allow the discloser to perform their duties from another location, reassign the discloser to another role at the same level, make other modifications to the discloser's workplace or the way they perform their work duties, or reassign or relocate other staff involved in the disclosable matter);

(f) how the entity will ensure that management are aware of their responsibilities to:

(i) maintain the confidentiality of a disclosure;

(ii) address the risks of isolation or harassment;

(iii) manage conflicts; and

(iv) ensure fairness when managing the performance of, or taking other management action relating to, a discloser;

(g) procedures on how a discloser can lodge a complaint if they have suffered detriment, and the actions the entity will take in response to such complaints (e.g. the complaint could be investigated as a separate matter by an officer who is not involved in dealing with disclosures and the investigation findings will be provided to the board or audit or risk committee); and

(h) the specific interventions the entity will take to protect a discloser if detriment has already occurred (e.g. the entity could investigate and address the detrimental conduct—such as by taking disciplinary action—or the entity could:

(i) allow the discloser to take extended leave;

(ii) develop an alternative career development plan for the discloser, including new training and career opportunities; or

(iii) the entity could offer compensation or other remedies.

Note: Research indicates that disclosers in entities that conduct risk assessments and proactively manage and prevent the risk of detriment receive better treatment and better outcomes—see J Olsen and AJ Brown, *Preventing detrimental whistleblowing outcomes: The value of risk assessment and proactive management* in AJ Brown (ed) *Whistleblowing: New rules, new policies, new vision (Work-in-progress research from the Whistling While They Work 2 Project)* (PDF 4.38 MB), Griffith University, November 2018. ASIC is a member of the Whistling While They Work 2 research project.

RG 000.121 In addition, the policy should explain that a discloser may seek independent legal advice or contact regulatory bodies, such as ASIC or APRA, if they believe they have suffered detriment.

Good practice guidance

RG 000.122 It is good practice for an entity to establish a risk assessment framework and procedures for assessing and controlling the risk of detriment.

RG 000.123 The framework and procedures should cover risk identification, risk analysis and evaluation, risk control and risk monitoring.

RG 000.124 An entity could gather information from a discloser about:

(a) the risk of their identity becoming known;

(b) who they fear might cause detriment to them;

(c) whether there are any existing conflicts or problems in the work place; and

(d) whether there have already been threats to cause detriment.

RG 000.125 An entity could also assess whether anyone may have a motive to cause detriment.

RG 000.126 Each risk should be analysed. The likelihood of each risk and the severity of the consequences should be evaluated. In addition, strategies should be developed and implemented to prevent or contain the risks.

RG 000.127 If an anonymous disclosure is made, the entity should conduct a risk assessment to assess whether the discloser's identity can be readily identified or may become apparent during an investigation.

RG 000.128 As the risk of detriment may increase or change as an investigation progresses, and even after an investigation is finalised, it is good practice to monitor and reassess the risk of detriment.

RG 000.129 An entity should keep appropriate records of its risk assessments and risk control plans.

Handling and investigating a disclosure

RG 000.130 An entity's whistleblower policy must include information about how it will investigate disclosures that qualify for protection: see s1317AI(5)(d).

RG 000.131 The policy should outline the steps the entity will take after it receives a disclosure. It should explain that the entity will need to assess each disclosure to determine whether:

(a) it falls within the entity's policy; and

(b) a formal, in-depth investigation is required.

RG 000.132 An entity should ensure the confidentiality of its disclosure handling and investigation process. It should also ensure appropriate records and documentation for each step in the process are maintained.

RG 000.133 An entity's whistleblower policy should include information about who will be responsible for handling and investigating a disclosure relating to its managing director, chief executive officer, whistleblower protection officer, whistleblower investigation officer, or a director. For example, the policy may state that such disclosures will be directed immediately to the chair of the audit or risk committee.

Process for investigating a disclosure

RG 000.134 An entity's policy should provide transparency about the entity's investigation process and timeframe.

RG 000.135 It should provide an overview of the different steps involved in investigating a disclosure, while acknowledging that the process may vary depending on the nature of the disclosure.

RG 000.136 The policy should explain that if an investigation is required, the entity will need to determine:

(a) the nature and scope of the investigation;

(b) the person(s) within and/or outside the entity that should lead the investigation;

(c) the nature of any technical, financial or legal advice that may be required to support the investigation; and

(d) the timeframe for the investigation.

RG 000.137 An entity's policy should acknowledge the limitations of the entity's investigation process. It should explain that the entity may not be able to undertake an investigation if it is not able to contact the discloser (e.g. if a disclosure is made anonymously and the discloser has refused or omitted to provide a means of contacting them).

RG 000.138 The policy should also explain that without the discloser's consent, the entity cannot disclose information that is contained in a disclosure as part of its investigation process—unless:

(a) the information does not include the discloser's identity;

(b) the entity removes information relating to the discloser's identity or other information that is likely to lead to the identification of the discloser (e.g. the discloser's name, position title and other identifying details); and

(c) it is reasonably necessary for investigating the issues raised in the disclosure.

Note: See s1317AAE(4) of the Corporations Act.

Good practice guidance

RG 000.139 To protect a discloser's identity from being revealed and to protect them from detriment, an entity could investigate a disclosure by conducting a broad review on the subject matter or the work area disclosed. In addition, it could investigate an anonymous disclosure, even if it cannot get in contact with the discloser, if the discloser has provided sufficient information to the entity and the entity removes information that is likely to lead to the identification of the discloser.

RG 000.140 We encourage entities to follow best practice in investigations. The investigation should be thorough, objective, fair and independent, while preserving the confidentiality of the investigation.

RG 000.141 To ensure fairness and independence, investigations need to be independent of the discloser, the individuals who are the subject of the disclosure, and the department or business unit involved.

RG 000.142 We also encourage entities to undertake investigations jointly with an external investigation firm, if required (e.g. when additional specialist skills or expertise are necessary).

Process for keeping a discloser informed

RG 000.143 An entity's whistleblower policy should state that each disclosure will be acknowledged within a reasonable period after the disclosure is received, if the discloser can be contacted (including through anonymous channels).

RG 000.144 The entity should provide disclosers with updates at various stages—for example when the investigation process has begun, while the investigation is in progress and after the investigation has been finalised. The policy should indicate how frequently a discloser will receive an update while an investigation is ongoing (e.g. once a quarter). It should also include the method for updating a discloser.

RG 000.145 Keeping a discloser informed and updated will provide them with assurance that the entity is taking their disclosure seriously.

How the investigation findings will be documented, reported internally and communicated to the discloser

RG 000.146 An entity's whistleblower policy should outline how the findings from an investigation will be documented and reported to those responsible for oversight of the policy, while preserving confidentiality: see RG 000.100–RG 000.107. It should also indicate the information the discloser will receive at the end of the investigation.

Good practice guidance

RG 000.147 It is good practice for an entity's policy to provide an avenue for review, if the discloser is not satisfied with the outcome of the investigation. The policy should provide information about the entity's review process. The review should be conducted by an officer who is not involved in handling and investigating disclosures. In addition, the review findings should be provided to the board or audit or risk committee.

RG 000.148 An entity's policy could include a statement outlining that the entity is not obliged to reopen an investigation and that it can conclude a review if it finds that the investigation was conducted properly, or new information is either not available or would not change the findings of the investigation.

RG 000.149 The policy could also include a statement advising that a discloser may lodge a complaint with a regulator, such as ASIC or APRA, if they are not satisfied with the outcome of the entity's investigation.

Ensuring fair treatment of individuals mentioned in a disclosure

RG 000.150 An entity's whistleblower policy must include information about how the entity will ensure the fair treatment of its employees who are mentioned in a disclosure that qualifies for protection, including those who are the subject of a disclosure: see s1317AI(5)(e). For example, the policy should explain that:

(a) disclosures will be handled confidentially, when it is practical and appropriate in the circumstances;

(b) each disclosure will be assessed and may be the subject of an investigation;

(c) the objective of an investigation is to determine whether there is enough evidence to substantiate or refute the matters reported; and

(d) an employee who is the subject of a disclosure will be advised about:

(i) the subject matter of the disclosure as and when required by principles of natural justice and procedural fairness, and prior to any actions being taken—for example, if the disclosure is to be the subject of an investigation or if the disclosure is serious and needs to be referred to ASIC, APRA or the Federal Police; and

(ii) the outcome of the investigation (but they will not be provided with a copy of the investigation report).

Good practice guidance

RG 000.151 It is good practice for an entity's whistleblower policy to state that, when an investigation needs to be undertaken, the process will be thorough, objective, fair and independent.

RG 000.152 The policy could refer to support services (e.g. counselling) that can be accessed by its employees.

Ensuring the policy is easily accessible

Disclosers within the entity

RG 000.153 An entity's whistleblower policy must cover information about how the policy will be made available to the entity's officers and employees: see s1317AI(5)(f).

RG 000.154 We expect an entity to take steps to ensure its whistleblower policy is widely disseminated to and easily accessible by its officers and employees. An entity should, for example:

(a) hold staff briefing sessions and/or smaller team meetings;

(b) make the policy accessible on the staff intranet or other communication platform;

(c) post information on staff noticeboards;

(d) set out the policy in the employee handbook; and

(e) incorporate the policy in employee induction information packs and training for new starters.

Upfront and ongoing education and training

RG 000.155 An entity should conduct upfront and ongoing education and training regarding its whistleblower policy, processes and procedures. The training should be provided to every employee.

RG 000.156 It is important that all levels of management within an entity, particularly line managers, receive appropriate training in how to effectively deal with disclosures.

RG 000.157 Entities should ensure that its eligible recipients receive training in the entity's processes and procedures for receiving and handling disclosures, including training relating to confidentiality and the prohibitions against detrimental conduct.

RG 000.158 Specialist training should be provided to staff members who have specific responsibilities under the policy.

RG 000.159 An entity should also inform its external eligible recipients (e.g. its auditor and actuary) about their obligations under the Corporations Act.

RG 000.160 Australian entities with overseas-based related entities need to ensure that people in their overseas-based operations also receive appropriate training, since disclosures made to the entity's overseas-based eligible recipients and disclosures about the entity's overseas-based entities and their officers and employees may qualify for protection.

Good practice guidance

RG 000.161 It is good practice for an entity's management to actively and regularly promote the entity's whistleblower policy. This may help demonstrate management's commitment to protect and support disclosers, and to identify and address wrongdoing promptly.

RG 000.162 It is also good practice for an entity to conduct regular training to ensure that the entity's whistleblower policy, processes and procedures stay fresh in the minds of the entity's employees, managers and staff members who have specific responsibilities under the policy.

RG 000.163 The employee training could include:

(a) the key arrangements of the entity's whistleblower policy, processes and procedures, including:

  (i) practical examples of disclosable matters;

  (ii) practical information on how to make a disclosure; and

  (iii) advice on how disclosers can seek further information about the policy if required.

(b) information related to protecting and supporting disclosers, including:

  (i) the measures the entity has in place for protecting and supporting disclosers;

  (ii) practical working examples of conduct that may cause detriment to a discloser; and

(iii) the consequences for engaging in detrimental conduct.

(c) information about matters that are not covered by the entity's policy, including:

(i) practical examples of the types of matters that are not covered by the entity's policy;

(ii) information on the entity's other policies (e.g. on bullying and harassment, workplace health and safety, grievance and code of conduct matters); and

(iii) information on how and where employees can report general employee feedback or personal work-related grievances.

RG 000.164 The management training could cover the entity's commitment and obligations to protecting disclosers of wrongdoing. It could also cover how the entity's whistleblower policy interacts with the entity's other policies (e.g. on bullying and harassment). It is important for the training to be incorporated as part of the entity's management competency training.

Disclosers outside the entity

RG 000.165 To ensure disclosers outside an entity can access the entity's whistleblower policy, the policy should be available on the entity's external website.

Monitoring and reporting on the effectiveness of the policy

Good practice guidance

RG 000.166 It is good practice for an entity's whistleblower policy to include a statement about its commitment to monitoring the effectiveness of its policy, processes and procedures.

RG 000.167 It is also good practice for an entity to have mechanisms in place for monitoring the effectiveness of its whistleblower policy and ensuring compliance with its legal obligations.

RG 000.168 An entity should have oversight arrangements for ensuring its board or audit or risk committee are kept informed about the effectiveness of the entity's policy, processes and procedures—and can intervene where necessary—while preserving confidentiality: see RG 000.100–RG 000.107.

RG 000.169 In addition, there should be a mechanism to enable the entity's board or the audit or risk committee to be notified immediately, if a disclosure relates to serious misconduct.

RG 000.170 Periodic reports (e.g. quarterly reports) could be submitted to the entity's board or the audit or risk committee on the following, when it is not likely to lead to the identification of a discloser:

(a) the subject matter of each disclosure;

(b) the status of each disclosure;

(c) for each disclosure, the type of person who made the disclosure (e.g. employee or supplier) and their status (e.g. whether they are still employed or contracted by the entity);

(d) the action taken for each disclosure;

(e) how each disclosure was finalised;

(f) the timeframe for finalising each disclosure; and

(g) the outcome of each disclosure.

RG 000.171 Statistics on the following could also be included in the periodic reports:

(a) the timeframe between receiving a disclosure and responding to a discloser, including the time taken to respond to subsequent messages from a discloser;

(b) the timeframe between receiving a disclosure and assessing whether a disclosure should be investigated;

(c) the timeframe between commencing and finalising an investigation; and

(d) how frequently communications are made with a discloser.

RG 000.172 The statistics could be compared to the timeframes outlined in the entity's policy and procedures for handling and investigating disclosures: see RG 000.134.

RG 000.173 The report could also include statistics on the total number of reports received, including:

(a) the number of reports made through each of the different options available for making a disclosure under the entity's policy;

(b) the types of matters reported; and

(c) reports provided by line of business, department, country, office or location.

RG 000.174 In addition, the report could also include measures on employees' understanding of the policy. This information could be gathered through:

(a) surveying a sample of staff after the entity initially implements its whistleblower policy;

(b) having conversations with a sample of employees; or

(c) monitoring the proportion of disclosures that relate to matters covered by its policy, against those that fall outside the policy—a high

percentage of disclosures that fall outside the policy would suggest that employees may be confused about what to report as well as where to report general employee feedback or personal work-related grievances.

RG 000.175 Monitoring employees' understanding on a periodic basis may help the entity to determine where there are knowledge gaps in their employees' understanding of its whistleblower policy. It may also help the entity to enhance and improve its ongoing education, training and management communication about the policy.

RG 000.176 An entity that has authorised an independent whistleblowing service provider for receiving disclosures could consider benchmarking its statistics against the statistics of other entities, if available through its independent whistleblowing service provider.

RG 000.177 It is important for an entity's board or audit or risk committee to ensure that the broader trends and themes and/or emerging risks highlighted by the disclosures made under its whistleblower policy are addressed and mitigated by the entity as part of its risk management and corporate governance work plans.

Reviewing and updating the policy

Good practice guidance

RG 000.178 It is good practice for an entity's whistleblower policy to include a brief statement outlining the entity's commitment to reviewing and updating its policy, processes and procedures. This may provide assurance to disclosers about the entity's commitment to ensuring the policy is operating effectively and commitment to identifying and rectifying issues.

RG 000.179 It is also good practice for an entity to review its whistleblower policy, processes and procedures on a periodic basis (e.g. every two years). It should also implement changes to rectify the issues it has identified from its review in a timely manner.

RG 000.180 An entity should ensure that any updates to its whistleblower policy, processes and procedures following a review are widely disseminated to, and easily accessible by, individuals covered by the policy. When necessary (e.g. if there has been a change to the disclosure procedures), the entity should provide targeted communications and training to all employees and eligible recipients, and additional specialist training to staff members who have specific roles and responsibilities under the policy.

RG 000.181 In reviewing the policy, processes and procedures, an entity could consider which aspects worked well and did not work well since they were last reviewed. Some issues to consider include whether:

(a) the scope and application of the policy are appropriate, particularly if there have been changes to the entity's business;

(b) the policy, processes and procedures are helpful and easy to understand;

(c) the policy, processes and procedures reflect current legislation and regulations, and current developments and best practice for managing disclosures; and

(d) the entity's handling of disclosures and its protections and support for disclosers need to be improved.

RG 000.182 An entity could consult with and seek feedback from its employees about the effectiveness of its whistleblower policy, processes and procedures.

C Additional good practice guidance on establishing, implementing and maintaining a whistleblower policy

Key points

This section provides additional good practice guidance on establishing, implementing and maintaining a whistleblower policy, which is not mandatory.

We have provided good practice guidance on:

- fostering a whistleblowing culture (see RG 000.183–RG 000.186);
- ensuring the privacy and security of personal information (see RG 000.187–RG 000.189);
- drafting the policy (see RG 000.190–RG 000.193); and
- other whistleblowing principles and standards (see RG 000.194–RG 000.196)

Fostering a whistleblowing culture

RG 000.183 It is important for entities to develop and maintain a culture of ethical conduct, and ensure the culture is cascaded throughout their organisation. When an entity's employees have a clear understanding of what represents ethical conduct, it will be easier to identify wrongdoing.

RG 000.184 It is also important for entities to create a positive and open environment where employees feel they can come forward to make a disclosure. A positive and open work environment may also help eliminate the negative connotations associated with whistleblowing.

RG 000.185 An entity's culture is strongly influenced by its leadership team. Senior leadership should be clearly committed to supporting the entity's whistleblower policy. In addition, an entity's leadership should demonstrate this in practice by ensuring disclosures are taken seriously and acted on immediately, wrongdoing is addressed promptly, disclosers are provided with adequate protections and support, and early interventions are made to protect disclosers from detriment.

RG 000.186 All levels of management, particularly line managers, play a critical role in creating an ethical culture and a positive and open environment for employees.

Ensuring the privacy and security of personal information

RG 000.187 Entities need to ensure they have appropriate information technology resources and organisational measures for securing the personal information they receive, handle and record as part of their whistleblower policy. Due to the sensitivity of the information, any leaks or unauthorised disclosure (including from malicious cyber activity) may have adverse consequences for the disclosers, the individuals who are the subject of disclosures and the entity.

RG 000.188 The *Privacy Act 1988* (Privacy Act) regulates the handling of personal information about individuals. It includes 13 Australian Privacy Principles (APPs), which set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information (including sensitive information). Entities regulated under the Privacy Act are required to notify affected individuals and the Office of the Australian Information Commissioner about a data breach, if it is likely to result in serious harm to individuals whose personal information is involved in the breach.

> Note: The Privacy Act defines 'personal information' as information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable—see s6(1) of the Privacy Act.

RG 000.189 We encourage entities to consult the APPs and other relevant industry, government and technology-specific standards, guidance and frameworks on data security to help safeguard their information.

Drafting of the policy

RG 000.190 The way an entity drafts its whistleblower policy and procedures will influence how its employees comprehend, retain and implement the policy and procedures.

RG 000.191 As the users of a whistleblower policy may have different requirements and needs, an entity should consider them when planning and developing the document.

RG 000.192 It is good practice for an entity's whistleblower policy to cater to the different users of the policy. For example, it should include employees based at the entity's head office and employees working at the entity's 'factory floor'.

RG 000.193 It is also good practice for an entity's whistleblower policy to be clear and easy to understand for the users of the document. The policy may be easier to understand if it:

(a) uses plain English and avoids legal or industry jargon;

(b) adopts a simple structure, including a contents list and clear headings; and

(c) includes diagrams and/or flowcharts explaining the whistleblowing processes and procedures, where possible.

Other whistleblowing principles and standards

RG 000.194 Entities may consider the below whistleblowing standard and guideline when establishing, implementing and maintaining their whistleblower policy.

Australian standards

RG 000.195 Australian Standard AS 8004–2003 *Corporate governance—Whistleblower protection programs for entities*, which has been withdrawn, was the standard for the implementation and handling of whistleblowing schemes by private sector organisations; it was developed and published by Standards Australia. It is intended to be revised.

International standards

RG 000.196 International Standard ISO 37002 *Whistleblowing management systems—Guidelines* is currently being developed by the International Organization for Standardization (ISO). The international standard is scheduled for completion by the end of 2021.

Key terms

Term	Meaning in this document
ACNC Act	*Australian Charities and Not-for-profits Commission Act 2012*
APPs	Australian Privacy Principles
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
ASX Corporate Governance Principles and Recommendations	The Principles and Recommendations set out recommended corporate governance practices for entities listed on the ASX. The fourth edition comes into force for financial years commencing on or after 1 January 2020
company limited by guarantee	A company where the liability of its members is limited to the respective amounts that the members have undertaken to contribute to the property of the company if it is wound up Note: See s9 of the Corporations Act.
Corporations Act	*Corporations Act 2001*, including regulations made for the purposes of that Act
detriment	Has the meaning given in s1317ADA of the Corporations Act
detrimental conduct	Conduct, or a threat to engage in conduct, that causes detriment to a discloser
director	Has the meaning given in s9 of the Corporations Act
disclosable matter	Information to which the whistleblower protections apply Note: See RG 000.39–RG 000.40 and s1317AA of the Corporations Act.
discloser	An individual who discloses wrongdoing or an eligible whistleblower
disclosure	A disclosure of information relating to wrongdoing or a disclosable matter
eligible recipient	An individual who can receive a disclosure Note: See s1317AAC(1)–(2) of the Corporations Act.
eligible whistleblower	An individual to whom the whistleblower protections apply Note: See RG 000.32–RG 000.33 and s1317AAA of the Corporations Act.

Term	Meaning in this document
emergency disclosure	The disclosure of information to a journalist or parliamentarian, where the discloser has reasonable grounds to believe that the information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment. The disclosure must meet a number of other criteria to qualify Note: See RG 000.70 and s1317AAD(2) of the Corporations Act.
entity	A public company, large proprietary company or proprietary company that is a trustee of a registrable superannuation entity that must have a whistleblower policy. Note: See s1317AI(1)–(3) of the Corporations Act.
journalist	Has the meaning given in s1317AAD(3) of the Corporations Act
large proprietary company	A proprietary company that qualifies as a large proprietary company under the Corporations Act Note: See RG 000.6 and s45A(3) and the Corporations Amendment (Proprietary Company Thresholds) Regulations 2019.
legal practitioner	Means a duly qualified legal practitioner and, in relation to a person, such a practitioner acting for the person
listed	Has the meaning given in s9 of the Corporations Act
officer	Has the meaning given in s9 of the Corporations Act
parliamentarian	A member of the Commonwealth, state or territory parliaments Note: See s1317AAD(1)(f) and 1317AAD(2)(d) of the Corporations Act.
personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether: • true or not; and • recorded in a material form or not Note: See s6(1) of the Privacy Act.
personal work-related grievance	A disclosure that relates to the discloser's current or former employment, which has implications for the discloser personally, but does not: • have any other significant implications for the entity (or another entity); or • relate to conduct, or alleged conduct, about a disclosable matter Note: See s1317AADA(2) of the Corporations Act.
Privacy Act	*Privacy Act 1988*

Term	Meaning in this document
proprietary company	A company that is registered as, or that converts to, a proprietary company under the Corporations Act Note: See s45A of the Corporations Act.
Pt 9.4AAA (for example)	A part of the Corporations Act (in this example, numbered 9.4AAA)
public company	A company other than a proprietary company Note: See s9 of the Corporations Act.
public interest disclosure	The disclosure of information to a journalist or a parliamentarian, where the discloser has reasonable grounds to believe that making a further disclosure of the information is in the public interest. The disclosure must meet a number of other criteria to qualify Note: See RG 000.69 and s1317AAD(1) of the Corporations Act.
registrable superannuation entity	A regulated superannuation fund, an approved deposit fund or a pooled superannuation trust, but not a self-managed superannuation fund Note: See s10 of the SIS Act.
related body corporate	A body corporate that is a: • holding company of another body corporate; or • subsidiary of another body corporate; or • subsidiary of a holding company of another body corporate Note: See s50 of the Corporations Act.
RG 51 (for example)	An ASIC regulatory guide (in this example numbered 51)
s1317AI (for example)	A section of the Corporations Act (in this example numbered 1317AI), unless otherwise specified
senior manager	In relation to a corporation, a person (other than a director or secretary of the corporation) who: • makes or participates in making decisions that affect the whole, or a substantial part, of the business of the entity; or • has the capacity to affect significantly the entity's financial standing. They are generally a senior executive within the entity Note: See s9 of the Corporations Act.
SIS Act	*Superannuation Industry (Supervision) Act 1993*
strict liability	There are no fault elements for any of the physical elements of the offence

Term	Meaning in this document
trustee	A body corporate that is a trustee of a fund, scheme or trust Note: See s10 of the SIS Act.
whistleblower	A discloser who has made a disclosure that qualifies for protection under the Corporations Act Note: See s1317AA, s1317AAA, s1317AAC, s1317AAD.
whistleblower investigation officer	The role under an entity's whistleblower policy that is responsible for investigating disclosures
whistleblower protection officer	The role under an entity's whistleblower policy that is responsible for protecting or safeguarding disclosers and ensuring the integrity of the reporting mechanism
Whistleblower Protections Act	*Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019*
Whistleblower Protections Bill	Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2018

Related information

Headnotes

detrimental conduct, discloser, disclosure, eligible whistleblowers, eligible recipients, large proprietary companies, protection, public companies, registrable superannuation entities, whistleblower policy, whistleblowing

Regulatory guides

RG 51 *Applications for relief*

Information sheets

INFO 238 *Whistleblower rights and protections*

INFO 239 *How ASIC handles whistleblower reports*

Legislation

ACNC Act, Div 60

Australian Federal Police Act 1979

Corporations Act, Pt 9.4AAA, s9, 45A(2), 45B, 1311(1), 1317AA, 1317AAA, 1317AAC, 1317AAD, 1317AADA, 1317AAE, 1317AB(1), 1317AC, 1317AD, 1317AE(3)(b), 1317AI, 1317AJ

Fair Work Act

Privacy Act 1988, s6(1)

SIS Act

Taxation Administration Act 1953

Whistleblower Protections Act

Whistleblower Protections Bill (Revised Explanatory Memorandum)

Other documents

AJ Brown and SA Lawrence, *Strength of organisational whistleblowing processes—Analysis from Australia & New Zealand: Further results: Whistling While They Work 2* (PDF 757 KB), July 2017.

J Olsen and AJ Brown, *Preventing detrimental whistleblowing outcomes: the value of risk assessment and proactive management* in AJ Brown (ed) *Whistleblowing: New rules, new policies, new vision (Work-in-progress research from the Whistling While They Work 2 Project)* (PDF 4.38 MB), Griffith University, November 2018.