



ASIC
Australian Securities &
Investments Commission

REGULATORY GUIDE 270

Whistleblower policies

November 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 a whistleblower policy that complies with their legal obligations. It also contains our good practice guidance on implementing and maintaining a whistleblower policy.

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 regulatory guide was issued in November 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.

This guide includes examples to help entities comply with their obligations; they are not exhaustive.

Contents

A	Overview	4
	The importance of whistleblower policies	4
	Entities that must have a whistleblower policy	5
	Requirement to have a whistleblower policy	6
	Complying with the requirements	7
	Summary of our guidance	7
	Our regulatory powers	12
B	Guidance on establishing a whistleblower policy	13
	Approach to our guidance	13
	Purpose of the policy	15
	Who the policy applies to	16
	Matters the policy applies to	18
	Who can receive a disclosure	22
	How to make a disclosure	26
	Legal protections for disclosers	27
	Support and practical protection for disclosers	31
	Handling and investigating a disclosure	34
	Ensuring fair treatment of individuals mentioned in a disclosure	38
	Ensuring the policy is easily accessible	39
C	Good practice guidance on implementing and maintaining a whistleblower policy	42
	Fostering a whistleblowing culture	42
	Roles and responsibilities under a policy	43
	Ensuring the privacy and security of personal information	44
	Monitoring and reporting on the effectiveness of the policy	44
	Reviewing and updating the policy	46
	Key terms	47
	Related information	51

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 a whistleblower policy that complies with the obligations under the Corporations Act.

We have also included some good practice tips and good practice guidance—which are 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 270.1 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 270.2 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 270.3 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 1: See s1317AI of the Corporations Act.

Note 2: In this guide, references to sections (s) and parts (Pts) are to the Corporations Act, unless otherwise specified.

RG 270.4 It is important to note that the whistleblower protections in Pt 9.4AAA are available to any discloser who makes a disclosure that qualifies for protection, regardless of whether the entity that is the subject of the disclosure must have a whistleblower policy.

Public companies

RG 270.5 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 270.6 All large proprietary companies must have a whistleblower policy: see s1317AI(2).

RG 270.7 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 270.8 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 270.9 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 270.10 The information in this guide will also help entities that would like to establish mechanisms for managing disclosures on a voluntary basis, since they are required to manage whistleblowing in accordance with the Corporations Act: see RG 270.4.

Requirement to have a whistleblower policy

RG 270.11 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 270.12 An entity's whistleblower policy should also include information about the protections provided in the tax whistleblower regime under Part IVD of the *Taxation Administration Act 1953* (Taxation Administration Act): see the [Revised Explanatory Memorandum](#) to the Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2018 (Whistleblower Protections Bill). We have included references to the Taxation Administration Act in this regulatory guide, where relevant. For further information about the protections under the tax whistleblower regime, see the webpage of the Australian Taxation Office (ATO) 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 270.13 To ensure entities have a whistleblower policy that sufficiently meets the objectives set out in RG 270.1–RG 270.2, we expect entities to:
- (a) establish a 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 that 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.
- RG 270.14 An entity’s board is ultimately responsible for the entity’s whistleblower policy, as part of the entity’s broader risk management and corporate governance framework. It is important for an entity’s board (either directly or through its audit or risk committee) to ensure that the broader trends, themes and/or emerging risks highlighted by the disclosures made under its policy are addressed and mitigated by the entity as part of its risk management and corporate governance work plans.

Summary of our guidance

- RG 270.15 In Section B, we provide guidance on *establishing* a whistleblower policy. Section B includes:
- (a) the matters that must be addressed by an entity’s whistleblower policy;
 - (b) examples of content for a whistleblower policy, which entities can adapt to their circumstances; and
 - (c) some good practice tips, which are contained in grey boxes—the good practice tips are not mandatory.
- RG 270.16 For a summary of Section B, see Table 1.
- RG 270.17 In Section C, we provide good practice guidance on *implementing and maintaining* a whistleblower policy. This guidance is not mandatory. For a summary, see Table 2.

Table 1: Summary of our guidance on establishing a whistleblower policy

Component	Guidance (relating to the requirements in s1317AI(5))	More information	Good practice tips (non-mandatory)
Purpose of the policy (see s1317AI)	The policy must include a brief explanation about the purpose of the policy.	RG 270.39– RG 270.40	Good practice tip 1: State the importance of the entity's whistleblower policy
Who the policy applies to (see s1317AI(5)(a))	An entity's whistleblower policy must 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 must set out the criteria for a discloser to qualify for protection as a whistleblower under the Corporations Act.	RG 270.41– RG 270.46	Good practice tip 2: Encourage those who are aware of wrongdoing to speak up
Matters the policy applies to (see s1317AI(5)(a))	An entity's whistleblower policy must identify the types of wrongdoing that can be reported (i.e. 'disclosable matters'), based on the entity's business operations and practices. In addition, the policy must outline the types of matters that are not covered by the policy (e.g. personal work-related grievances). The policy must state that disclosures that are not about 'disclosable matters' do not qualify for protection under the Corporations Act.	RG 270.47– RG 270.63	Good practice tip 3: Provide information about how to internally raise grievances that are not covered by the policy Good practice tip 4: Include a statement discouraging deliberate false reporting
Who can 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 receive a disclosure that qualifies for protection—that is: <ul style="list-style-type: none"> • 'eligible recipients'; • legal practitioners; • regulatory bodies and other external parties; and • journalists and members of Commonwealth, state or territory parliaments (parliamentarians), under certain circumstances. The policy must also include information about who a discloser can contact to obtain additional information before making a disclosure.	RG 270.64– RG 270.78	Good practice tip 5: Encourage disclosures to the entity in the first instance Good practice tip 6: Use independent whistleblowing service providers when necessary Good practice tip 7: Provide advice about how to make a disclosure to an external party

Component	Guidance (relating to the requirements in s1317AI(5))	More information	Good practice tips (non-mandatory)
How to make a disclosure (see s1317AI(5)(b))	<p>An entity's whistleblower policy must include information about how to make a disclosure.</p> <p>The policy must 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.</p> <p>The policy must include information about how to access each option, along with the relevant instructions.</p> <p>The policy must advise that disclosures can be made anonymously and still be protected under the Corporations Act.</p>	RG 270.79– RG 270.86	Not applicable
Legal protections for disclosers (see s1317AI(5)(a))	<p>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:</p> <ul style="list-style-type: none"> • identity protection (confidentiality); • protection from detrimental acts or omissions; • compensation and remedies; and • civil, criminal and administrative liability protection. 	RG 270.87– RG 270.105	Not applicable
Support and practical protection for disclosers (see s1317AI(5)(c))	<p>An entity's whistleblower policy must outline the entity's measures for supporting disclosers and protecting disclosers from detriment in practice.</p> <p>The policy must provide examples of how the entity will, in practice:</p> <ul style="list-style-type: none"> • protect the confidentiality of a discloser's identity; and • protect disclosers from detrimental acts or omissions. 	RG 270.106– RG 270.110	<p>Good practice tip 8: Explain how the entity will protect confidentiality when initially dealing with a discloser</p> <p>Good practice tip 9: Establish processes for assessing and controlling the risk of detriment</p>

Component	Guidance (relating to the requirements in s1317AI(5))	More information	Good practice tips (non-mandatory)
Handling and investigating a disclosure (see s1317AI(5)(d))	<p>An entity's whistleblower policy must include information about how the entity will investigate disclosures that qualify for protection.</p> <p>The policy must outline the key steps the entity will take after it receives a disclosure, including how it:</p> <ul style="list-style-type: none"> • investigates a disclosure; • keeps a discloser informed; and • documents, reports internally and communicates to the discloser the investigation findings. 	RG 270.111– RG 270.124	<p>Good practice tip 10: Determine whether the location and time are appropriate for receiving a disclosure</p> <p>Good practice tip 11: Focus on the substance, rather than the motive, of disclosures</p> <p>Good practice tip 12: Outline the factors that the entity will consider when investigating a disclosure</p> <p>Good practice tip 13: Ensure investigations follow best practice</p> <p>Good practice tip 14: Provide an avenue for review</p>
Ensuring fair treatment of individuals mentioned in a disclosure (see s1317AI(5)(e))	<p>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.</p>	RG 270.125– RG 270.127	Not applicable
Ensuring the policy is easily accessible (see s1317AI(5)(f))	<p>An entity's whistleblower policy must cover how the policy will be made available to the entity's officers and employees.</p> <p>It must 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).</p> <p>An entity should make its policy available on its external website.</p>	RG 270.128– RG 270.139	<p>Good practice tip 15: Demonstrate the entity's commitment to the policy by promoting it actively and regularly</p> <p>Good practice tip 16: Provide upfront and ongoing training to all staff</p>

Table 2: Summary of our good practice guidance on implementing and maintaining a whistleblower policy

Component	Good practice guidance (non-mandatory)	More information
Fostering a whistleblowing culture	<p>It is important for an entity to create a positive and open environment:</p> <ul style="list-style-type: none"> • so that employees feel they can come forward to make a disclosure; and • to help eliminate the negative connotations associated with whistleblowing. <p>The senior leadership team plays an important role in demonstrating the entity's commitment to its whistleblower policy.</p>	RG 270.140– RG 270.143
Roles and responsibilities	<p>It is good practice for an entity to allocate key roles and responsibilities under its whistleblower policy.</p> <p>An entity could create new roles. Alternatively, the responsibilities could be integrated into existing roles. Staff members may hold more than one role, provided it does not result in conflicts of interest.</p>	RG 270.144– RG 270.146
Ensuring the privacy and security of personal information	<p>It is good practice for an entity to have appropriate information technology resources and organisational measures for securing the personal information they receive, handle and record as part of their whistleblower policy.</p> <p>It is important for an entity to consult the Australian Privacy Principles (APPs) and other relevant industry, government and technology-specific standards, guidance and frameworks on data security to help safeguard their information.</p>	RG 270.147– RG 270.149
Monitoring and reporting on the effectiveness of the policy	<p>It is important for an entity to have mechanisms in place for monitoring the effectiveness of its whistleblower policy and ensuring compliance with its legal obligations.</p> <p>An entity could set up:</p> <ul style="list-style-type: none"> • 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 when necessary—while preserving confidentiality; • a mechanism to enable matters to be escalated to the entity's board or the audit or risk committee, when required; and • periodic reporting to the board or audit or risk committee. 	RG 270.150– RG 270.157
Reviewing and updating the policy	<p>It is good practice for an entity to review its whistleblower policy, processes and procedures on a periodic basis (e.g. every two years). It is also good practice to rectify any issues identified in the review in a timely manner.</p>	RG 270.158– RG 270.160

Our regulatory powers

Power to grant relief by legislative instrument

- RG 270.18 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 270.19 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).

Companies that are not-for-profits or charities

- RG 270.20 We have granted relief to small not-for-profits or charities—that is, companies limited by guarantee that have revenue (or consolidated revenue, if that applies) for the financial year of less than \$1 million: see [ASIC Corporations \(Whistleblower Policies\) Instrument 2019/1146](#).
- RG 270.21 The revenue threshold for the relief is consistent with:
- (a) the threshold for the full financial reporting and auditing requirements that apply to companies limited by guarantee under the Corporations Act; and
 - (b) the threshold for large charities registered with the Australian Charities and Not-for-profits Commission.
- RG 270.22 We have provided this relief to take a similar approach for proprietary companies and public companies, while accounting for the differences in the regulatory requirements that apply to these corporate structures. Small proprietary companies are not required to have a whistleblower policy: see s1317AI(2). However, s1317AI(1) requires all public companies, including small companies limited by guarantee, to have a policy.

Penalty for non-compliance

- RG 270.23 ASIC is responsible for administering the whistleblower protection provisions in the Corporations Act, including the whistleblower policy requirement. Periodically, ASIC will conduct surveillance activities to ensure compliance with the obligations and pursue non-compliance in accordance with our enforcement approach and operational priorities. For further information, see [Information Sheet 151 ASIC's approach to enforcement](#) (INFO 151).
- RG 270.24 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 for individuals and companies (currently \$12,600), enforceable by ASIC: see s1317AI(4) and 1311(1).

B Guidance on establishing a whistleblower policy

Key points

This section provides guidance to help entities establish a whistleblower policy that complies with their legal obligations. We have included examples of content for a whistleblower policy where relevant. Entities should adapt the examples to their circumstances when establishing their whistleblower policy.

This section also includes a series of 'good practice tips'. Each of the good practice tips is contained in a grey box. It is not mandatory for entities to follow these tips when establishing their whistleblower policy.

Approach to our guidance

Matters that must be addressed by an entity's whistleblower policy

- RG 270.25 This section covers the following matters that must be addressed by an entity's whistleblower policy:
- (a) purpose of the policy (see RG 270.39–RG 270.40);
 - (b) who the policy applies to (see RG 270.41–RG 270.46);
 - (c) matters the policy applies to (see RG 270.47–RG 270.63);
 - (d) who can receive a disclosure (see RG 270.64–RG 270.78);
 - (e) how to make a disclosure (see RG 270.79–RG 270.86);
 - (f) legal protections for disclosers (see RG 270.87–RG 270.105);
 - (g) support and practical protection for disclosers (see RG 270.106–RG 270.110);
 - (h) handling and investigating a disclosure (see RG 270.111–RG 270.124);
 - (i) ensuring fair treatment of individuals mentioned in a disclosure (see RG 270.125–RG 270.127); and
 - (j) ensuring the policy is easily accessible (see RG 270.128–RG 270.139).
- RG 270.26 The matters we have included reflect all stages of the whistleblowing process:
- (a) receiving a disclosure (including providing advice to individuals who are considering making a disclosure);
 - (b) assessing how a discloser should be supported and protected;
 - (c) assessing whether a disclosure should be investigated;

- (d) undertaking an investigation;
- (e) supporting and protecting a discloser during and after the investigation;
- (f) communicating with a discloser, including about the outcome of an investigation; and
- (g) ensuring oversight and monitoring by the entity's board.

RG 270.27 Our guidance 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 270.28 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 et al, [Clean as a whistle: A five step guide to better whistleblowing policy and practice in business and government—Key findings and actions of Whistling While They Work 2](#) (PDF 4.95MB), Griffith University, August 2019. ASIC is a member of the Whistling While They Work 2 research project.

Structuring, drafting and presenting a whistleblower policy

RG 270.29 This section is also intended to provide entities with a potential structure from which to develop their own whistleblower policy. Entities may wish to use the list of 'matters that must be addressed by an entity's whistleblower policy' in RG 270.25 as headings for the different sections of their policy.

RG 270.30 Entities, particularly smaller entities, may wish to refer to relevant materials on whistleblowing from ASIC, the Australian Prudential Regulation Authority (APRA) or the Australian Taxation Office (ATO) in their policy.

RG 270.31 The way an entity drafts its whistleblower policy (including any processes and procedures it may have to support the policy) will influence how its employees comprehend and retain the policy.

RG 270.32 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 270.33 This section uses the language of the legal requirements under the Corporations Act to help entities establish a whistleblower policy that complies with their

legal obligations. To ensure an entity's whistleblower policy is clear and easy to understand for the users of the document, we encourage entities to:

- (a) use plain English and avoid legal or industry jargon;
- (b) adopt a simple structure, including a contents list and clear headings; and
- (c) include diagrams and/or flowcharts, where relevant.

RG 270.34 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 in preventing and responding to misconduct.

RG 270.35 Regardless of how an entity structures, drafts and presents its whistleblower policy, we expect the content to cover the information required under s1317AI(5) and this guidance.

Examples of content for a whistleblower policy

RG 270.36 This section includes examples of content for a whistleblower policy, including examples that relate to measures and/or mechanisms for receiving, handling, and investigating disclosures. Entities should adapt these examples to their circumstances when establishing their whistleblower policy.

Good practice tips

RG 270.37 This section also includes 'good practice tips' relating to some of the matters that must be addressed by an entity's whistleblower policy.

RG 270.38 Each of the good practice tips is contained in a grey box. Entities are not required to follow the tips when establishing their whistleblower policy. We encourage entities to incorporate them into their whistleblower policy and whistleblower processes and procedures, if they are relevant to their circumstances and/or would benefit the users of their policy.

Purpose of the policy

RG 270.39 Section 1317AI requires entities to have a whistleblower policy.

RG 270.40 To assist users of an entity's whistleblower policy, the policy must include a brief explanation about the purpose of the policy.

Examples: Purpose of a policy

An entity's policy may include the following as the purpose of its policy (where applicable):

- to encourage more disclosures of wrongdoing;
- to help deter wrongdoing, in line with the entity's risk management and governance framework;
- to ensure individuals who disclose wrongdoing can do so safely, securely and with confidence that they will be protected and supported;
- to ensure disclosures are dealt with appropriately and on a timely basis;
- to provide transparency around the entity's framework for receiving, handling and investigating disclosures;
- to support the entity's values, code of conduct and/or ethics policy;
- to support the entity's long-term sustainability and reputation;
- to meet the entity's legal and regulatory obligations; and
- to align with the ASX Corporate Governance Principles and Recommendations (which applies to listed companies) and relevant standards.

Good practice tip 1: State the importance of the entity's whistleblower policy

An entity's policy may explain that the entity's whistleblower policy is an important tool for helping the entity to identify wrongdoing that may not be uncovered unless there is a safe and secure means for disclosing wrongdoing.

Good practice tip 2: Encourage those who are aware of wrongdoing to speak up

An entity's policy may include specific statements encouraging the entity's employees (and non-employees) who are aware of possible wrongdoing to have the confidence to speak up.

Who the policy applies to

- RG 270.41 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 270.42 To assist users of an entity's whistleblower policy, the policy must 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').

- RG 270.43 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 (e.g. current and former employees who are permanent, part-time, fixed-term or temporary, interns, secondees, managers, and directors);
 - (b) a supplier of services or goods to the entity (whether paid or unpaid), including their employees (e.g. current and former contractors, consultants, service providers and business partners);
 - (c) an associate of the entity; and
 - (d) a relative, dependant or spouse of an individual in RG 270.43(a)–RG 270.43(c) (e.g. relatives, dependants or spouse of current and former employees, contractors, consultants, service providers, suppliers and business partners).

Note: See s1317AAA of the Corporations Act. Also see s14ZZU of the Taxation Administration Act.

- RG 270.44 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 270.44(a)–RG 270.44(c).

Note: See s1317AAA.

- RG 270.45 An entity's policy must 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, 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, 1317AAA, 1317AAC and 1317AAD of the Corporations Act. 'Disclosable matters' and 'eligible recipients' are explained in RG 270.50–RG 270.57 and RG 270.67–RG 270.71. Also see s14ZZT, 14ZZU and 14ZZV of the Taxation Administration Act. Disclosures pertaining to tax matters are referred to as 'disclosures qualifying for protection'. Disclosures qualifying for protection may be made to the ATO, an eligible recipient or a legal practitioner under the Taxation Administration Act.

RG 270.46 In practice, the types of disclosers who are covered by an entity's policy will depend on the entity's business operations, practices and organisational structure and set-up. Whistleblower protection legislation varies across jurisdictions and multinational entities should take this into account when establishing their whistleblower policy.

Matters the policy applies to

RG 270.47 Section 1317AI(5)(a) requires an entity's whistleblower policy to include information about the protections under the Corporations Act that are available to disclosers who qualify for protection as a whistleblower.

RG 270.48 To assist users of an entity's whistleblower policy, the policy must identify the types of wrongdoing that can be reported under the policy, based on the entity's business operations and practices. In addition, the policy must outline the types of matters that are not covered by the policy.

RG 270.49 An entity's policy must state that disclosures that are not about disclosable matters do not qualify for protection under the Corporations Act (or the Taxation Administration Act, where relevant). The policy may note that such disclosures may be protected under other legislation, such as the *Fair Work Act 2009* (Fair Work Act).

Note 1: An entity may choose to establish a whistleblower policy that covers a broader range of reports about issues and concerns (e.g. breaches of the entity's code of conduct) as part of the entity's 'speak up culture'. However, the policy must clearly explain that disclosers who submit reports about issues and concerns will not be able to access the whistleblower protections under the Corporations Act (or the Taxation Administration Act, where applicable).

Note 2: Disclosable matters are explained in RG 270.50–RG 270.57.

Disclosable matters

RG 270.50 An entity's policy must cover the types of disclosures that qualify for protection under the Corporations Act (i.e. 'disclosable matters'): see s1317AA.

RG 270.51 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) of the Corporations Act. Also see s14ZZT of the Taxation Administration Act. To qualify for protection under the tax whistleblower regime, the eligible whistleblower must have reasonable grounds to suspect that the information indicates misconduct or an improper state of affairs or circumstances in relation to tax affairs of the entity. The eligible whistleblower may assist the eligible recipient to perform its functions or duties in relation to those tax affairs.

- RG 270.52 The term ‘misconduct’ is defined in s9 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. 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 business behaviour and practices that may cause consumer harm.
- RG 270.53 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.
- RG 270.54 Disclosable matters also involve information about an entity in RG 270.51, 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 270.54(a)(i)–RG 270.54(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). Rather, they make clear that certain forms of conduct qualify for protection. Also see s14ZZT of the Taxation Administration Act. Disclosures pertaining to tax matters are referred to as ‘disclosures qualifying for protection’.

- RG 270.55 An entity's whistleblower policy must include examples of disclosable matters that relate specifically to the entity's business operations and practices.

Examples: Types of wrongdoing that could be covered by an entity's policy

An entity's policy may cover the following types of wrongdoing (where relevant to its business operations and practices):

- illegal conduct, such as theft, dealing in, or use of illicit drugs, violence or threatened violence, and criminal damage against property;
- fraud, money laundering or misappropriation of funds;
- offering or accepting a bribe;
- financial irregularities;
- failure to comply with, or breach of, legal or regulatory requirements; and
- 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 270.56 The policy should highlight that disclosable matters include conduct that may not involve a contravention of a particular law. It should also highlight 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 270.57 An entity's policy must state that a discloser can still qualify for protection even if their disclosure turns out to be incorrect.

Personal work-related grievances

- RG 270.58 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 1317AC.
- RG 270.59 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 270.51 and RG 270.54).

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

- RG 270.60 An entity's policy must clarify that disclosures relating to personal work-related grievances do not qualify for protection under the Corporations Act. The policy should explain the meaning of 'personal work-related grievance' by including some examples.

- RG 270.61 Section 1317AADA(2) includes specific examples of grievances that may be personal work-related grievances. These examples include:
- (a) an interpersonal conflict between the discloser and another employee;
 - (b) a decision that does not involve a breach of workplace laws;
 - (c) a decision about the engagement, transfer or promotion of the discloser;
 - (d) a decision about the terms and conditions of engagement of the discloser; or
 - (e) a decision to suspend or terminate the engagement of the discloser, or otherwise to discipline the discloser.
- RG 270.62 The policy must outline when a disclosure about, or including, a personal work-related grievance still qualifies for protection.
- RG 270.63 A personal work-related grievance may still qualify for protection if:
- (a) it 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 270.96–RG 270.97); or
 - (d) the discloser seeks legal advice or legal representation about the operation of the whistleblower protections under the Corporations Act (see RG 270.72).

Good practice tip 3: Provide information about how to internally raise grievances that are not covered by the policy

An entity's policy may 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 to resolve their personal work-related grievance.

Discouraging false reporting

Good practice tip 4: Include a statement discouraging deliberate false reporting

An entity's policy may include a statement discouraging deliberate false reporting (i.e. a report that the discloser knows to be untrue). 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).

Who can receive a disclosure

RG 270.64 Section 1317AI(5)(b) requires an entity's whistleblower policy to include information about:

- (a) who can receive disclosures that qualify for protection; and
- (b) how disclosures may be made.

RG 270.65 To assist users of an entity's whistleblower policy, the policy must identify the types of people within and outside the entity who can receive disclosures that qualify for protection.

RG 270.66 Taking into consideration that some disclosers may wish to seek additional information before formally making their disclosure, an entity's whistleblower policy must also include information about how a discloser can obtain additional information (e.g. by contacting the entity's whistleblower protection officer or equivalent (see RG 270.145) or an independent legal adviser).

Eligible recipients in relation to the entity

RG 270.67 An entity's policy must explain the role of 'eligible recipients'—that is, to receive disclosures that qualify for protection. The policy must 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 (or the Taxation Administration Act, where relevant).

RG 270.68 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 s1317AAC(1) of the Corporations Act. As set out at paragraph 2.60 in the [Revised Explanatory Memorandum](#) to the Whistleblower Protections Bill, 'a reference to an auditor in the Bill includes both internal and external auditors'. Also see s14ZZT(2) of the Taxation Administration Act.

RG 270.69 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. Also see s14ZZV of the Taxation Administration Act.

- RG 270.70 Generally, an ‘officer’ includes a director or company secretary of an entity.
- RG 270.71 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 tip 5: Encourage disclosures to the entity in the first instance

An entity’s policy may encourage its employees and external disclosers to make a disclosure to one of the entity’s internal or external eligible recipients in the first instance.

The policy could include a statement that the entity would like to identify and address wrongdoing as early as possible. 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.

The policy may 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 270.73.

Legal practitioners

- RG 270.72 An entity’s policy must highlight 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 that the legal practitioner concludes that a disclosure does not relate to a ‘disclosable matter’): see s1317AA(3).

Note: See s14ZZT(3) of the Taxation Administration Act.

Good practice tip 6: Use independent whistleblowing service providers when necessary

A smaller entity may consider authorising an independent whistleblowing service provider as an eligible recipient for directly receiving disclosures (i.e. by its employees and non-employees), where it is financially viable for them to do so. The entity may also consider engaging an independent investigation firm. Alternatively, the entity may consider referring disclosers to the entity’s external eligible

recipients (e.g. auditor or actuary to provide better protections to disclosers).

A larger entity may also consider authorising an independent whistleblowing service provider as an eligible recipient for directly receiving some of its 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.

By authorising an independent whistleblower service provider, an entity may encourage more disclosures since disclosers can:

- make their disclosure anonymously, confidentially, and outside of business hours;
- receive updates on the status of their disclosure while retaining anonymity; and
- provide additional information to the entity while retaining anonymity.

Responsibility for outsourced functions

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. The entity should also ensure that it has mechanisms for monitoring the services outsourced.

Regulatory bodies and other external parties

RG 270.73 An entity's policy must state 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).

Note: See s14ZZT(1) of the Taxation Administration Act. A discloser can make a disclosure to the ATO and qualify for protection.

Good practice tip 7: Provide advice about how to make a disclosure to an external party

An entity's policy may provide advice about how an employee can make a disclosure outside the entity and qualify for protection.

The policy could include links to whistleblowing information provided by ASIC, APRA or the ATO, such as ASIC [Information Sheet 239](#) *How ASIC handles whistleblower reports* (INFO 239).

Public interest disclosures and emergency disclosures

- RG 270.74 An entity's policy must state that disclosures can be made to a journalist or parliamentarian under certain circumstances and qualify for protection: see s1317AAD.
- RG 270.75 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 270.75(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). A Commonwealth body had not yet been prescribed when this regulatory guide was published.

- RG 270.76 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 270.76(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). A Commonwealth body has not been prescribed at the time of publication of this guidance.

- RG 270.77 The policy must highlight that it is important for the discloser to understand the criteria for making a public interest or emergency disclosure. It should clarify

that a disclosure must have previously been made to ASIC, APRA or a prescribed body and written notice provided to the body to which the disclosure was made. It should also clarify that, in the case of a public interest disclosure, at least 90 days must have passed since the previous disclosure.

- RG 270.78 An entity's policy should state that a discloser should contact an independent legal adviser before making a public interest disclosure or an emergency disclosure.

How to make a disclosure

- RG 270.79 An entity's whistleblower policy must include information about how to make a disclosure: see s1317AI(5)(b).
- RG 270.80 To assist users of an entity's whistleblower policy, the policy must include a range of internal and external disclosure options. The options should allow for disclosures to be made anonymously and/or confidentially, securely and outside of business hours.
- RG 270.81 Providing an external option will help ensure that 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. In addition, it better enables the entity's non-employees (e.g. former employees and current and former suppliers) to make a disclosure to the entity.
- RG 270.82 An entity's policy must include information about how to access each option, along with the relevant instructions.

Examples: Information about accessing internal and external disclosure options

An entity's policy may include the following information, depending on the options available to disclosers:

- information on how to contact the entity's eligible recipients in person or through post or email;
- the telephone number for the entity's internal whistleblower hotline or the entity-authorised external hotline; and
- a link to the entity-authorised external whistleblower platform.

Anonymous disclosures

- RG 270.83 An entity's policy must include a statement advising that disclosures can be made anonymously and still be protected under the Corporations Act: see s1317AAE.

RG 270.84 The policy must state 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 state that a discloser can refuse to answer questions that they feel could reveal their identity at any time, including during follow-up conversations. In addition, it should include a suggestion 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.

Note: See note under s14ZZT of the Taxation Administration Act.

RG 270.85 In practice, 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.

RG 270.86 To assist users of an entity's whistleblower policy, the policy must outline the entity's measures and/or mechanisms for protecting anonymity.

Examples: Measures and/or mechanisms for protecting anonymity

An entity's policy may refer to the following measures and/or mechanisms for protecting anonymity (where applicable):

- communication with disclosers will be through anonymous telephone hotlines and anonymised email addresses; and
- a discloser may adopt a pseudonym for the purpose of their disclosure—this may be appropriate in circumstances where the discloser's identity is known to their supervisor, the whistleblower protection officer or equivalent (see RG 270.145) but the discloser prefers not to disclose their identity to others.

Legal protections for disclosers

RG 270.87 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).

Note: Where applicable, an entity's policy should include information about the protections under the Taxation Administration Act.

RG 270.88 The policy must cover the following protections:

- (a) identity protection (confidentiality) (see RG 270.90–RG 270.94);
- (b) protection from detrimental acts or omissions (see RG 270.95–RG 270.101);
- (c) compensation and other remedies (see RG 270.102–RG 270.103); and
- (d) civil, criminal and administrative liability protection (see RG 270.104–RG 270.105).

RG 270.89 The policy must highlight 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 270.90 An entity's policy must explain the entity's legal obligations to protect the confidentiality of a discloser's identity.

RG 270.91 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).

Note: See s14ZZW of the Taxation Administration Act.

RG 270.92 The exception to RG 270.91 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.

Note: See s14ZZW(2) of the Taxation Administration Act.

RG 270.93 A person can disclose the information contained in a disclosure with or 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 270.94 An entity's policy must highlight 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 270.92–RG 270.93. It should include information about how a discloser can lodge a complaint with the entity about a breach of confidentiality. It should also state that a discloser may lodge a complaint with a regulator, such as ASIC, APRA or the ATO, for investigation.

Protection from detrimental acts or omissions

- RG 270.95 An entity's whistleblower policy must explain the legal protections for protecting a discloser, or any other person, from detriment in relation to a disclosure.
- RG 270.96 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 270.97 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. Also see s14ZZY of the Taxation Administration Act.

- RG 270.98 The policy should provide examples of detrimental conduct that are prohibited under the law, without deterring employees from making disclosures.
- RG 270.99 Section 1317ADA defines detrimental conduct as including the following:
- (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: Also see s14ZZZAA of the Taxation Administration Act.

- RG 270.100 The policy should also provide examples of actions that are not detrimental conduct.

Examples: Actions that are not detrimental conduct

An entity's policy may include the following as examples of actions that are not detrimental conduct (where relevant):

- administrative action that is reasonable for the purpose of protecting a discloser from detriment (e.g. moving a discloser who has made a disclosure about their immediate work area to another office to prevent them from detriment); and
- managing a discloser's unsatisfactory work performance, if the action is in line with the entity's performance management framework.

RG 270.101 An entity should ensure that a discloser understands the reason for the entity's administrative or management action.

Compensation and other remedies

RG 270.102 An entity's policy must 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 take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

Note: See s1317AD of the Corporations Act. Also see s14ZZZA of the Taxation Administration Act.

RG 270.103 The policy should include a statement encouraging disclosers to seek independent legal advice.

Civil, criminal and administrative liability protection

RG 270.104 An entity's policy must state 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 270.105 The policy should state 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).

Support and practical protection for disclosers

- RG 270.106 An entity's policy must include information about how it will support disclosers and protect disclosers from detriment: see s1317AI(5)(c).
- RG 270.107 Although an entity's whistleblower policy may refer to or include a link to document(s) outlining the entity's more detailed processes and procedures for supporting and protecting disclosers, the policy must cover the information required under s1317AI(5)(c).

Identity protection (confidentiality)

- RG 270.108 An entity's policy must provide examples of how the entity will, in practice, protect the confidentiality of a discloser's identity.

Examples: Measures and/or mechanisms for protecting the confidentiality of a discloser's identity

An entity's policy may include the following measures and/or mechanisms for protecting the confidentiality of a discloser's identity (where applicable).

Reducing the risk that the discloser will be identified from the information contained in a disclosure

The policy may set out that:

- all personal information or reference to the discloser witnessing an event will be redacted;
- the discloser will be referred to in a gender-neutral context;
- where possible, the discloser will be contacted to help identify certain aspects of their disclosure that could inadvertently identify them; and
- disclosures will be handled and investigated by qualified staff.

Secure record-keeping and information-sharing processes

The policy may set out that:

- all paper and electronic documents and other materials relating to disclosures will be stored securely;
- access to all information relating to a disclosure will be limited to those directly involved in managing and investigating the disclosure;
- only a restricted number of people who are directly involved in handling and investigating a disclosure will be made aware of a discloser's identity (subject to the discloser's consent) or information that is likely to lead to the identification of the discloser;
- communications and documents relating to the investigation of a disclosure will not be sent to an email address or to a printer that can be accessed by other staff; and
- each person who is involved in handling and investigating a disclosure will be reminded about the confidentiality requirements, including that an unauthorised disclosure of a discloser's identity may be a criminal offence.

Good practice tip 8: Explain how the entity will protect confidentiality when initially dealing with a discloser

An entity's policy may outline that the entity's whistleblower protection officer, or equivalent (see RG 270.145) is responsible for discussing the entity's measures for ensuring confidentiality of their identity.

The policy may highlight that, in practice, people may be able to guess the discloser's identity if:

- the discloser has previously mentioned to other people that they are considering making a disclosure;
- the discloser is one of a very small number of people with access to the information; or
- the disclosure relates to information that a discloser has previously been told privately and in confidence.

Protection from detrimental acts or omissions

RG 270.109 An entity's policy must outline examples of how the entity will, in practice, protect disclosers from detriment.

Examples: Measures and/or mechanisms for protecting disclosers from detriment

An entity's policy may refer to the following measures and mechanisms for protecting disclosers from detrimental acts or omissions (where applicable):

- 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), which will commence as soon as possible after receiving a disclosure;
- support services (including counselling or other professional or legal services) that are available to disclosers;
- strategies to help a discloser minimise and manage stress, time or performance impacts, or other challenges resulting from the disclosure or its investigation;
- actions for protecting a discloser from risk of detriment—for example, 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;
- processes for ensuring that management are aware of their responsibilities to maintain the confidentiality of a disclosure, address the risks of isolation or harassment, manage conflicts, and ensure fairness when managing the performance of, or taking other management action relating to, a discloser;
- procedures on how a discloser can lodge a complaint if they have suffered detriment, and the actions the entity may 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

- interventions for protecting a discloser if detriment has already occurred—for example, the entity could investigate and address the detrimental conduct, such as by taking disciplinary action, or the entity could allow the discloser to take extended leave, develop a career development plan for the discloser that includes new training and career opportunities, or 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 AJ Brown et al, [Clean as a whistle: A five step guide to better whistleblowing policy and practice in business and government—Key findings and actions of Whistling While They Work 2](#) (PDF 4.95MB), Griffith University, August 2019. ASIC is a member of the Whistling While They Work 2 research project.

RG 270.110 In addition, the policy should state that a discloser may seek independent legal advice or contact regulatory bodies, such as ASIC, APRA or the ATO, if they believe they have suffered detriment.

Good practice tip 9: Establish processes for assessing and controlling the risk of detriment

It is important for an entity to establish processes for assessing and controlling the risk of detriment. The processes could be based upon the entity's existing risk management framework.

It is also important for an entity to keep appropriate records of its risk assessments and risk control plans.

Steps in assessing and controlling the risk of detriment

- **Risk identification:** Assessing whether anyone may have a motive to cause detriment—information could be gathered from a discloser about:
 - the risk of their identity becoming known;
 - who they fear might cause detriment to them;
 - whether there are any existing conflicts or problems in the work place; and
 - whether there have already been threats to cause detriment.
- **Risk analysis and evaluation:** Analysing and evaluating the likelihood of each risk and evaluating the severity of the consequences.
- **Risk control:** Developing and implementing strategies to prevent or contain the risks—for anonymous disclosures, it may be worthwhile assessing whether the discloser's identity can be readily identified or may become apparent during an investigation.
- **Risk monitoring:** Monitoring and reassessing the risk of detriment where required—the risk of detriment may increase or change as an investigation progresses, and even after an investigation is finalised.

Handling and investigating a disclosure

- RG 270.111 An entity's whistleblower policy must include information about how the entity will investigate disclosures that qualify for protection: see s1317AI(5)(d).
- RG 270.112 To assist users of an entity's whistleblower policy, the policy must provide transparency about how it will handle and investigate disclosures, including timeframes for handling and investigating disclosures.
- RG 270.113 An entity must ensure the confidentiality of its disclosure handling and investigation process. It must also ensure appropriate records and documentation for each step in the process are maintained.
- RG 270.114 Although an entity's whistleblower policy may refer to or include a link to document(s) outlining the entity's more detailed processes and procedures for handling and investigating disclosures, the policy must cover the information required under s1317AI(5)(d).

Handling a disclosure

- RG 270.115 An entity's policy must outline the key steps the entity will take after it receives a disclosure.
- RG 270.116 The policy should state that the entity will need to assess each disclosure to determine whether:
- (a) it qualifies for protection; and
 - (b) a formal, in-depth investigation is required.

Good practice tip 10: Determine whether the location and time are appropriate for receiving a disclosure

It is important for an entity's eligible recipients to determine whether the location and time are appropriate:

- for the discloser to make their disclosure comfortably; and
- for ensuring the discloser is protected.

Good practice tip 11: Focus on the substance, rather than the motive, of disclosures

It is important for an entity to focus on the substance of a 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.

In circumstances where it may be unclear whether a disclosure qualifies for protection, an entity could elect to treat the discloser as though they were protected as a whistleblower under the Corporations Act (or the Taxation Administration Act, where relevant).

Investigating a disclosure

- RG 270.117 An entity's policy must outline the key steps involved in investigating a disclosure, including the timeframes, while acknowledging that the process may vary depending on the nature of the disclosure.
- RG 270.118 The policy should highlight that without the discloser's consent, the entity cannot disclose information that is likely to lead to the identification of the discloser 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. 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. Also see s14ZZW(3) of the Taxation Administration Act.

- RG 270.119 An entity's policy should acknowledge the limitations of the entity's investigation process. It should state 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 to provide, or has not provided, a means of contacting them).
- RG 270.120 In practice, an entity may investigate a disclosure by asking the discloser for consent to a limited disclosure (e.g. disclosure to the entity's whistleblower protection officer or equivalent and the entity's whistleblower investigation officer or equivalent). An entity may also 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.

Good practice tip 12: Outline the factors that the entity will consider when investigating a disclosure

An entity's whistleblower protection officer, or equivalent (see RG 270.145) may explain that if the entity determines that it will need to investigate a disclosure, the entity will need to determine:

- the nature and scope of the investigation;
- the person(s) within and/or outside the entity that should lead the investigation;
- the nature of any technical, financial or legal advice that may be required to support the investigation; and
- the timeframe for the investigation.

Good practice tip 13: Ensure investigations follow best practice

It is important for entities to follow best practice in investigations.

Investigations need to be objective, fair and independent, while preserving the confidentiality of the investigation.

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.

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

Keeping a discloser informed

RG 270.121 An entity's policy must state that a discloser will be provided with regular updates, if the discloser can be contacted (including through anonymous channels). The policy should acknowledge that the frequency and timeframe may vary depending on the nature of the disclosure.

RG 270.122 Keeping a discloser informed and updated during various stages of the investigation will provide a discloser with assurance that the entity is taking their disclosure seriously. It is important for the entity to ensure that anonymity is not compromised when providing regular updates.

Examples: Communicating with a discloser

An entity's policy may outline that the entity will acknowledge a discloser after receiving their disclosure.

In addition, the policy may state that the entity will provide updates to a discloser during the key stages, such as:

- when the investigation process has begun;
- while the investigation is in progress; and
- after the investigation has been finalised.

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

RG 270.123 An entity's policy must 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 270.90–RG 270.94. In addition, it should indicate the information the discloser will receive at the end of the investigation.

RG 270.124 The policy should clarify that the method for documenting and reporting the findings will depend on the nature of the disclosure. It should also clarify that there may be circumstances where it may not be appropriate to provide details of the outcome to the discloser.

Good practice tip 14: Provide an avenue for review

An entity's whistleblower policy may provide an avenue for reviewing whether the entity's policy, processes and procedures had been adhered to, if the discloser is not satisfied with the outcome of the investigation.

The policy could include information about the entity's review process. It could also 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. In addition, it could include a statement advising that a discloser may lodge a complaint with a regulator, such as ASIC, APRA or the ATO, if they are not satisfied with the outcome of the entity's investigation.

If an entity provides an avenue for review, it is good practice for the review to be conducted by an officer who is not involved in handling and investigating disclosures. It is also good practice to provide the review findings to the board or audit or risk committee.

Ensuring fair treatment of individuals mentioned in a disclosure

- RG 270.125 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).
- RG 270.126 Although an entity's whistleblower policy may refer to or include a link to document(s) outlining the entity's more detailed processes and procedures for ensuring fair treatment of individuals mentioned in a disclosure, the policy must cover the information required under s1317AI(5)(e).

Examples: Measures and/or mechanisms for ensuring fair treatment of individuals mentioned in a disclosure

An entity's policy may include the following measures and/or mechanisms for ensuring fair treatment of individuals mentioned in a disclosure (where applicable):

- disclosures will be handled confidentially, when it is practical and appropriate in the circumstances;
- each disclosure will be assessed and may be the subject of an investigation;
- the objective of an investigation is to determine whether there is enough evidence to substantiate or refute the matters reported;
- when an investigation needs to be undertaken, the process will be objective, fair and independent;
- an employee who is the subject of a disclosure will be advised about 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 will be the subject of an investigation; and
- an employee who is the subject of a disclosure may contact the entity's support services (e.g. counselling).

- RG 270.127 An entity may determine the most appropriate time to inform the individual who is the subject of a disclosure about the investigation, provided that they inform the individual before making any adverse finding against them. In some circumstances, informing the individual at an early stage of an investigation may compromise the effectiveness of the investigation, such as when there may be concerns that the individual may destroy information or the disclosure needs to be referred to ASIC, APRA, the ATO or the Federal Police.

Ensuring the policy is easily accessible

Disclosers within the entity

- RG 270.128 An entity's policy must cover information about how the policy will be made available to the entity's officers and employees: see s1317AI(5)(f).
- RG 270.129 We expect an entity to take steps to ensure that its whistleblower policy is widely disseminated to, and easily accessible by, its officers and employees.
- RG 270.130 Although an entity's whistleblower policy may include references and links to other relevant information (e.g. training packs), the policy must cover the information required under s1317AI(5)(f).

Examples: Methods for making a policy available

An entity's policy may include the following methods for making the policy available to the entity's officers and employees (where applicable):

- holding staff briefing sessions and/or smaller team meetings;
- posting the policy on the staff intranet or other communication platform;
- posting information on staff noticeboards;
- setting out the policy in the employee handbook; and
- incorporating the policy in employee induction information packs and training for new starters.

Good practice tip 15: Demonstrate the entity's commitment to the policy by promoting it actively and regularly

We encourage an entity's management to actively and regularly promote the entity's whistleblower policy. This may help demonstrate the entity's commitment to protect and support disclosers, and to identify and address wrongdoing promptly.

Upfront and ongoing education and training

- RG 270.131 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 270.132 Conducting regular training will help ensure the entity's policy, processes and procedures stay fresh in the minds of the entity's employees.
- RG 270.133 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 270.134 Specialist training should be provided to staff members who have specific responsibilities under the policy: see RG 270.145. For example, an entity's eligible recipients should 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 270.135 An entity should also inform its external eligible recipients (e.g. its auditor and actuary) about their obligations under the Corporations Act (and the Taxation Administration Act, where applicable).
- RG 270.136 Australian entities with overseas-based related entities need to ensure that people in their overseas-based operations also receive appropriate training. This is because 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.
- RG 270.137 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: see RG 270.158–RG 270.160. 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.

Good practice tip 16: Provide upfront and ongoing training to all staff

The employee training may include:

- the key arrangements of the entity's whistleblower policy, processes and procedures, including:
 - practical examples of disclosable matters;
 - practical information on how to make a disclosure; and
 - advice on how disclosers can seek further information about the policy if required.
- information related to protecting and supporting disclosers, including:
 - the measures the entity has in place for protecting and supporting disclosers;
 - practical working examples of conduct that may cause detriment to a discloser; and
 - the consequences for engaging in detrimental conduct.
- information about matters that are not covered by the entity's policy, including:
 - practical examples of personal work-related grievances;
 - information on the entity's other policies (e.g. on bullying and harassment, workplace health and safety, grievance and code of conduct matters);
- information on how and where employees can report general employee

feedback or personal work-related grievances; and

- practical examples of circumstances where disclosure has led to positive outcomes for the entity and the discloser.

The management training may cover the entity's commitment and obligations to protecting disclosers of wrongdoing. It may also cover how the entity's whistleblower policy interacts with the entity's other policies (e.g. on bullying and harassment). An entity may consider incorporating the training as part of the entity's management competency training.

Disclosers outside the entity

RG 270.138 To ensure disclosers outside an entity can access the entity's whistleblower policy, the policy should be available on the entity's external website.

RG 270.139 Where appropriate, an entity may exclude information that would not be useful or relevant to external disclosers or that would not be suitable for external publication (e.g. the names and contact phone numbers of internal eligible recipients for employees).

C Good practice guidance on implementing and maintaining a whistleblower policy

Key points

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

We have provided good practice guidance on:

- fostering a whistleblowing culture (see RG 270.140–RG 270.143);
- roles and responsibilities under a policy (see RG 270.144–RG 270.146);
- ensuring the privacy and security of personal information (see RG 270.147–RG 270.149);
- monitoring and reporting on the effectiveness of the policy (see RG 270.150–RG 270.157); and
- reviewing and updating the policy (see RG 270.158–RG 270.160).

Fostering a whistleblowing culture

- RG 270.140 It is important for an entity to create a positive and open environment where employees feel they can come forward to make a disclosure. A positive and open environment may also help eliminate the negative connotations associated with whistleblowing.
- RG 270.141 An entity's senior leadership team plays an important role in demonstrating the entity's commitment to its whistleblower policy. They can demonstrate their commitment in practice by ensuring:
- (a) disclosures are taken seriously and acted on immediately;
 - (b) wrongdoing is addressed promptly;
 - (c) disclosers are provided with adequate protections and support; and
 - (d) early interventions are made to protect disclosers from detriment.
- RG 270.142 It is important for an entity to develop and maintain a culture of ethical conduct, and ensure this culture flows through their organisation. When an entity's employees have a clear understanding of what represents ethical conduct, it will be easier to identify wrongdoing.
- RG 270.143 All levels of management, particularly line managers, play a critical role in creating an ethical culture and a positive and open environment for employees.

Roles and responsibilities under a policy

RG 270.144 It is good practice for an entity to allocate key roles and responsibilities under its whistleblower policy.

RG 270.145 Below is a list of roles and responsibilities that may help in supporting an entity's whistleblower policy:

- (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, 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) a role for supporting training, education and communications about the policy;
- (h) 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;
- (i) an officer responsible for periodically reviewing and updating the whistleblower policy, processes and procedures, and for implementing and overseeing any changes;
- (j) the owner of the whistleblower policy who is responsible for oversight and monitoring of the policy; and
- (k) 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 270.90–RG 270.94.

RG 270.146 An entity could create new roles. Alternatively, the responsibilities could be integrated into existing roles. Staff members may hold more than one role, provided that this does not result in conflicts of interest. For example, it is

important for an entity to enable its whistleblower protection officer and whistleblower investigation officer (or equivalent), to exercise independent judgement and have a mechanism through which they can escalate problems directly to the entity's board.

Ensuring the privacy and security of personal information

RG 270.147 It is good practice for an entity to 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 270.148 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 270.149 It is important for the entity to consult the APPs and other relevant industry, government and technology-specific standards, guidance and frameworks on data security to help safeguard their information.

Monitoring and reporting on the effectiveness of the policy

RG 270.150 It is important for an entity to have mechanisms in place for monitoring the effectiveness of its whistleblower policy and ensuring compliance with its legal obligations.

RG 270.151 An entity could set up 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 270.90–RG 270.94. It could also set up a mechanism to enable matters to be escalated to the entity's board or the audit or risk committee, where required.

- RG 270.152 It is good practice for an entity to provide periodic reports to the entity's board or the audit or risk committee. The reports could include the following information on individual disclosures received under the entity's policy, 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 270.153 The reports could also include the following statistics on the entity's handling of individual disclosures, including a comparison with the timeframes for handling and investigating disclosures outlined in the entity's policy (see RG 270.111–RG 270.124):
- (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;
 - (d) how frequently communications are made with a discloser; and
- RG 270.154 An entity could also report statistics on the total number of reports received, including:
- (i) the number of reports made through each of the different options available for making a disclosure under the entity's policy;
 - (ii) the types of matters reported; and
 - (iii) reports provided by line of business, department, country, office or location.
- RG 270.155 An entity could also monitor and measure its employees' understanding of the entity's whistleblower policy, processes and procedures on a periodic basis. This may help the entity to determine where there are gaps in their employees' understanding. It may also help the entity to enhance and improve its ongoing education, training and communication about the policy.

- RG 270.156 An entity could track employees' understanding of the policy 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 and the proportion of disclosures that are not covered by the policy—a high percentage of disclosures that are not covered 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 270.157 An entity that has authorised an independent whistleblowing service provider for receiving disclosures could also compare its statistics with the statistics of other entities, if available through its independent whistleblowing service provider.

Reviewing and updating the policy

- RG 270.158 It is good practice for an entity to review its whistleblower policy, processes and procedures on a periodic basis (e.g. every two years). It is also good practice to rectify any issues identified in the review in a timely manner.
- RG 270.159 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 270.160 An entity could consult with and seek feedback from its employees about the effectiveness of its whistleblower policy, processes and procedures.

Key terms

Term	Meaning in this document
APPs	Australian Privacy Principles
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
ASX Corporate Governance Principles and Recommendations	Recommended corporate governance practices for entities listed on the ASX Note: The fourth edition comes into force for financial years commencing on or after 1 January 2020.
ATO	Australian Taxation Office
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	<i>Corporations Act 2001</i> , including regulations made for the purposes of that Act
detriment	Has the meaning given in s1317ADA of the Corporations Act Note: Also see s14ZZZAA of the Taxation Administration 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 270.50–RG 270.57 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
disclosures qualifying for protection	Disclosures pertaining to tax matters are referred to as ‘disclosures qualifying for protection’ Note: See s14ZZT of the Taxation Administration Act.
eligible recipient	An individual who can receive a disclosure Note: See s1317AAC(1)–(2) of the Corporations Act. Also see s14ZZV of the Taxation Administration Act, which includes prescribed bodies.

Term	Meaning in this document
eligible whistleblower	<p>An individual to whom the whistleblower protections apply</p> <p>Note: See RG 270.43–RG 270.44 and s1317AAA of the Corporations Act. Also see s14ZZU of the Taxation Administration Act.</p>
emergency disclosure	<p>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</p> <p>Note: The disclosure must meet a number of other criteria to qualify. See RG 270.76 and s1317AAD(2) of the Corporations Act.</p>
entity	<p>A public company, large proprietary company or proprietary company that is a trustee of a registrable superannuation entity that must have a whistleblower policy</p> <p>Note: See s1317AI(1)–(3) of the Corporations Act.</p>
journalist	<p>Has the meaning given in s1317AAD(3) of the Corporations Act</p>
large proprietary company	<p>A proprietary company that qualifies as a large proprietary company under the Corporations Act</p> <p>Note: See RG 270.7 and s45A(3) and the Corporations Amendment (Proprietary Company Thresholds) Regulations 2019.</p>
legal practitioner	<p>Means a duly qualified legal practitioner and, in relation to a person, such a practitioner acting for the person</p>
listed	<p>Has the meaning given in s9 of the Corporations Act</p>
officer	<p>Has the meaning given in s9 of the Corporations Act</p>
parliamentarian	<p>A member of the Commonwealth, state or territory parliaments</p> <p>Note: See s1317AAD(1)(f) and 1317AAD(2)(d) of the Corporations Act.</p>
personal information	<p>Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether:</p> <ul style="list-style-type: none"> • true or not; and • recorded in a material form or not <p>Note: See s6(1) of the Privacy Act.</p>

Term	Meaning in this document
personal work-related grievance	<p>A disclosure that relates to the discloser's current or former employment, which has implications for the discloser personally, but does not:</p> <ul style="list-style-type: none"> • have any other significant implications for the entity (or another entity); or • relate to conduct, or alleged conduct, about a disclosable matter <p>Note: See s1317AADA(2) of the Corporations Act.</p>
Privacy Act	<i>Privacy Act 1988</i>
proprietary company	<p>A company that is registered as, or that converts to, a proprietary company under the Corporations Act</p> <p>Note: See s45A of the Corporations Act.</p>
Pt 9.4AAA (for example)	A part of the Corporations Act (in this example, numbered 9.4AAA)
public company	<p>A company other than a proprietary company</p> <p>Note: See s9 of the Corporations Act.</p>
public interest disclosure	<p>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.</p> <p>Note: See RG 270.75 and s1317AAD(1) of the Corporations Act.</p>
registrable superannuation entity	<p>A regulated superannuation fund, an approved deposit fund or a pooled superannuation trust, but not a self-managed superannuation fund</p> <p>Note: See s10 of the SIS Act.</p>
related body corporate	<p>A body corporate that is a:</p> <ul style="list-style-type: none"> • holding company of another body corporate; • subsidiary of another body corporate; or • subsidiary of a holding company of another body corporate <p>Note: See s50 of the Corporations Act.</p>
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

Term	Meaning in this document
senior manager	<p>In relation to a corporation, a person (other than a director or secretary of the corporation) who:</p> <ul style="list-style-type: none"> • 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 significantly affect the entity's financial standing. <p>They are generally a senior executive within the entity</p> <p>Note: See s9 of the Corporations Act.</p>
SIS Act	<i>Superannuation Industry (Supervision) Act 1993</i>
strict liability	An offence where there is no need for fault or intent in order for a person to be liable
tax affairs	<p>Affairs relating to any tax imposed by or under, or assessed or collected under, a law administered by the Commissioner of Taxation</p> <p>Note: See s14ZZT(4) of the Taxation Administration Act.</p>
Taxation Administration Act	<i>Taxation Administration Act 1953</i> , including regulations made for the purposes of that Act
trustee	<p>A body corporate that is a trustee of a fund, scheme or trust</p> <p>Note: See s10 of the SIS Act.</p>
whistleblower	<p>A discloser who has made a disclosure that qualifies for protection under the Corporations Act</p> <p>Note: See s1317AA, 1317AAA, 1317AAC, and 1317AAD of the Corporations Act. Also see s14ZZT, s14ZZY, s14ZZV of the Taxation Administration Act for a discloser that qualifies for protection under that Act.</p>
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 Bill	Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2018

Related information

Headnotes

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

Legislative instruments

ASIC Corporations (Whistleblower Policies) Instrument 2019/1146

Regulatory guides

[RG 51](#) *Applications for relief*

Information sheets

[INFO 238](#) *Whistleblower rights and protections*

[INFO 239](#) *How ASIC handles whistleblower reports*

Legislation

Australian Federal Police Act 1979

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

Fair Work Act

Privacy Act, s6(1)

Revised Explanatory Memorandum to the Whistleblower Protections Bill

SIS Act

Taxation Administration Act

Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019

Whistleblower Protections Bill

Other documents

Brown, AJ et al, [Clean as a whistle: A five step guide to better whistleblowing policy and practice in business and government—Key findings and actions of Whistling While They Work 2](#) (PDF 4.95MB), Griffith University, August 2019.