HOSTPLUS

Whistleblower Policy

Risk and Compliance

Policy Owner	Chief Risk Officer
Highest Approval Authority	Board of Directors
Last Approval Date	2 December 2025
Next Approval Date	2 December 2027

THAT'S A PLUS+

Table of Contents

1. Introduction

Host-Plus Pty Limited ("**Trustee**") as the Trustee of the Hostplus Superannuation Fund ("**Fund**") and the Hostplus Pooled Superannuation Trust ("**Hostplus PST**") (collectively, "**Hostplus**") recognises the importance of transparent whistleblower policies for good risk management and effective corporate governance. This Whistleblower Policy (the "**Policy**") is an important tool for Hostplus to identify wrongdoing that may not be uncovered unless there is a safe and secure means for disclosing wrongdoing.

Hostplus supports and protects staff who, on reasonable grounds and in good faith report instances of suspected Improper Conduct, including misconduct, an improper state of affairs or unethical, dishonest or illegal activity. Hostplus is committed to a "speak up" culture where concerns about misconduct can be raised safely and addressed promptly. This Policy explains how to report concerns, who can receive a report, how we protect reporters from detriment and keep identities confidential.

2. Definitions

The following terms have been defined for the purposes of this Policy.

Term	Definition
AFP	Means the Australian Federal Police.
APRA	Means the Australian Prudential Regulation Authority.
ASIC	Means the Australian Securities and Investment Commission.
ASIC Act	Means the *Australian Securities and Investment Commission Act 2001* (Cth).
Associate	Means any individual who is: • an associate within the meaning of the Corporations Act; or • if the disclosure relates to Hostplus' tax affairs, an associate within the meaning of section 318 of the Income Tax Assessment Act 1936 (Cth).
ATO	Means the Australian Taxation Office.
RCC	Means Hostplus' Board Risk and Compliance Committee.
AC	Means Hostplus' Board Audit Committee.
Corporations Act	*Corporations Act 2001* (Cth).
CPO	Means the Chief People Officer.
CRO	Means the Chief Risk Officer.
Custodian	Has the meaning given to it in the SIS Act.
Detriment	Has the meaning given to it in section 13.1 of this Policy.

Term	Definition
Disclosable Matters	A Disclosable Matter is a matter that an individual has reasonable grounds to suspect concerns Improper Conduct in relation to Hostplus which may be reported by Eligible Whistleblowers and protected under law and this Policy.
EAP	Means Hostplus' Employee Assistance Program.
Eligible Recipients	The internal and external personnel specified in section 10 to whom whistleblower disclosures must be made to qualify for protection under the law and this Policy.
Eligible Whistleblower	An individual qualifies as an Eligible Whistleblower and receives whistleblower protection under the law and this Policy, if the individual is or has been: • An officer or employee of Hostplus (including a Director or Company Secretary); • A supplier of services or goods to Hostplus (whether paid or unpaid) and employees of the supplier; • An associate of Hostplus; • A Trustee, Custodian or Investment Manager of Hostplus, including their employees and officers; • A supplier of services or goods to the Trustee, Custodian or Investment Manager, whether paid or unpaid, and employees of the supplier; • A relative, dependent or spouse of any person referred to above, or a dependent of such a person's spouse.
Emergency Disclosure	Has the meaning given to it in section 1317AAD of the Corporations Act.
Fund	Means Hostplus Superannuation Fund.
Hostplus	Means Host-Plus Pty Limited as the Trustee of the Fund and Hostplus PST.
Improper Conduct	Improper Conduct means a matter that may be reported by a Whistleblower in relation to Hostplus and includes misconduct or an improper state of affairs or circumstances (including in relation to the tax affairs of Hostplus or an associate). Refer to section 7 for examples of Improper Conduct.
Investment Manager	Has the meaning given to that term in the SIS Act.
Modern Slavery Act	Means the *Modern Slavery Act 2018* (Cth).
Personal Work-Related Grievance	Has the meaning given to that term in section 9 of this Policy.
Policy	Means this Whistleblower Policy.
PP&C	Means Hostplus' People, Performance and Culture team.
Public Interest Disclosure	Has the meaning given to that term in section 1317AAD of the Corporations Act.
Officer	Has the meaning given to that term in the Corporations Act.

Term	Definition
Reasonable Grounds	To access protections under the law and this Policy, the whistleblower must have 'Reasonable grounds' to believe that there has been Improper Conduct in relation to Hostplus. In this context, 'reasonable' means that a reasonable person in the whistleblower's position would also suspect the information indicates Improper Conduct. The term 'reasonable grounds to suspect' is based on the objective reasonableness of the reasons for the discloser's suspicion.
Registered tax agent or BAS agent	Has the meaning given to that term in the *Tax Agent Services Act 2009* (Cth).
SIS Act	Means the *Superannuation Industry (Supervision) Act 1993* (Cth).
Taxation Administration Act	Means the *Taxation Administration Act 1953* (Cth).
Trustee	Means Host-Plus Pty Limited as the Trustee of the Fund and Hostplus PST.
Whistleblower Laws	Means the Corporations Act and the Taxation Administration Act.
Whistleblowing	To 'blow the whistle' on someone is to alert a third party that another person has done, or is doing, something wrong, that is, to alert others to misconduct, dishonest or illegal activity.

3. Purpose

The protection of whistleblowers is linked to the overall protection and accountability of Hostplus as an organisation. Hostplus considers that a viable, published and well understood whistleblowing protection mechanism is vital to encourage the disclosure of information that may not otherwise be discovered. This serves to combat the disruptive effects that misconduct inevitably has on the structure and coherence of an organisation.

The purpose of this Policy is to:

- encourage the disclosure of wrongdoing and, in this way, deter wrongdoing;
- ensure individuals who disclose wrongdoing can do so safely and securely, and to provide them with information about how they will be protected and supported by Hostplus;
- provide information about Hostplus' processes for receiving, handling and investigating disclosures;
- ensure disclosures are dealt with appropriately and on a timely basis;
- tangibly support Hostplus' policies and values;
- support Hostplus' long-term sustainability and reputation; and
- meet Hostplus' legal and regulatory obligations and protect Hostplus' corporate reputation.

This Policy assists Hostplus to comply with relevant requirements of the enhanced whistleblowing protection laws by the Australian parliament, the Corporations Act and the Taxation Administration Act (together, the "**Whistleblower Laws**").

All Hostplus staff are encouraged to speak up if they become aware of wrongdoing. Hostplus has set out a Code of Conduct, which sets out principles for ethical behaviour designed to help Hostplus staff make informed choices about their behaviour. All staff (including Hostplus employees, CEO, managers, directors and contractors) must review and attest to the Code of Conduct at the time of hire and annually thereafter.

4. Scope

This Policy applies to Eligible Whistleblowers who may make a disclosure that qualifies for protection under the Whistleblower Laws.

If an individual is an Eligible Whistleblower and has made:

- a disclosure of information relating to a Disclosable Matter directly to an Eligible Recipient or to ASIC, APRA or another prescribed Commonwealth body;
- 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
- an Emergency Disclosure or Public Interest Disclosure,

then that individual will qualify for protection as a whistleblower under the Whistleblower Laws.

5. Relevant laws

The requirements in this Policy reflect the obligations and/or regulatory guidance contained in:

- the Corporations Act, part 9.4AAA;
- the Taxation Administration Act, part IVD; and
- ASIC Regulatory Guide 270 Whistleblower policies.

6. Related documents

This Policy should be read in conjunction with the following:

- Hostplus' Anti-Fraud, Scam and Corruption Policy;
- Hostplus' Code of Conduct;
- Hostplus' Privacy Policy;
- Hostplus' Modern Slavery Policy; and
- Hostplus' Key Guidelines to Corrective Action.

7. What matters should be reported? ("Disclosable Matters")

Whistleblowers may report on matters relating to Improper Conduct, as defined in section 2 above. Examples of Improper Conduct include:

Fraud, Dishonesty & Corruption

- Dishonest, fraudulent, corrupt or unlawful conduct;
- Negligence, default, breach of trust and breach of duty;
- Theft, misuse or embezzlement of assets (including cash and intellectual property);
- Misappropriation of funds or kickbacks, secret commissions, bribes;
- Falsification or misleading financial statements or records;
- Misleading or deceptive conduct, including improper accounting practices;
- Concealment of any misconduct;

Legal & Regulatory Breaches

- Breach of fiduciary duties or failure to act in the best interests of Hostplus or its employees;
- Willful or intentional violations of laws or regulations;
- Illegal conduct, such as theft, use of illicit drugs, violence or threatened violence, and criminal damage against property;
- Contravention of any law punishable by imprisonment of 12 months or more;
- Breach of laws applicable to Hostplus (e.g. Corporations Act, ASIC Act, SIS Act, Modern Slavery Act);

Policy & Governance Violations

- Breach of Hostplus policies that results in an improper state of affairs or harm (e.g. Code of Conduct, Conflicts Management Policy, Fit and Proper Policy, Modern Slavery Policy, Health & Safety Policy);
- Conduct resulting in a material mismanagement of Hostplus' assets or resources;
- Any other misconduct or improper state of affairs (excluding Personal Work-Related Grievances);

Ethical & Social Harm

- Conduct that poses a danger or significant risk to public safety or the stability of, or confidence in, the financial system;
- Workplace violence, bullying, harassment, coercion or discrimination;
- Modern slavery or human trafficking, including in Hostplus' supply chain;
- Victimisation of a potential or actual whistleblower;
- Systemic unethical behaviour or practices; and
- Any conduct causing or potentially causing significant harm or loss to Hostplus and its employees.

If an Eligible Whistleblower has Reasonable Grounds to suspect that information concerns Improper Conduct, such information will be a Disclosable Matter that may qualify for protection

under Whistleblower Laws. This definition is broad enough to include matters which could indicate a systemic issue that the relevant regulator should know about to properly perform its functions or a business practice that could cause a Hostplus employee or member harm.

This Policy also covers reporting on matters relating to conduct that involves:

- a breach of Hostplus' legislative or regulatory requirements; and/or
- a breach of Hostplus' internal policies, including the Modern Slavery Policy.

A disclosure does not need to include conduct involving contravention of a particular law to be a Disclosable Matter. A discloser may still qualify for protection even if their disclosure turns out to be incorrect. Whilst Hostplus encourages reports of suspected wrongdoing, any instances of deliberate false reports will not be protected under this policy and will be dealt with in accordance with Hostplus' Consequence Management Framework.

Modern slavery

Hostplus is committed to identifying and addressing all forms of modern slavery in its operations and supply chains. Employees, contractors, and other stakeholders are encouraged to report any concerns or suspicions regarding modern slavery practices, including forced labour, human trafficking, or exploitation.

Some modern slavery-related disclosures may qualify for whistleblower protection under the Whistleblower Laws if they involve criminal conduct or an "improper state of affairs" (e.g., systemic exploitation or concealment of slavery-like practices) related to Hostplus or are otherwise a Disclosable Matter. However, not all modern slavery disclosures are automatically protected under Whistleblower Laws. Each case must be assessed individually.

8. Reasonable Grounds for Disclosure

When making a disclosure, whistleblowers will be expected to have reasonable grounds to suspect the information being disclosed is true. A whistleblower will not be penalised if the information turns out to be incorrect. However, an individual must not make a report that they know is not true or is misleading.

Where it is found that an individual knowingly made a false report, this may be a breach of the Code of Conduct and will be considered a serious matter that may result in disciplinary action. There may also be legal consequences if an individual makes a knowingly false report.

9. What matters are not covered by the Whistleblower Policy?

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.

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 have any other significant implications for Hostplus or relate to any conduct, or alleged conduct, about a Disclosable Matter ("**Personal Work-Related Grievance**").

Personal Work-Related Grievances should be reported to your line manager or to the People, Performance and Culture (**PP&C**) team. Examples of grievances that may be Personal Work-Related Grievance include:

- An interpersonal conflict between the discloser and another employee;
- A decision relating to the engagement, transfer or promotion of the discloser;
- A decision relating to the terms and conditions of engagement of the discloser; or
- A decision to suspend or terminate the engagement of the discloser, or otherwise to discipline the discloser.

A Personal Work-Related Grievance may still qualify for protection if it also relates to a Disclosable Matter or in some other limited circumstances, for example if:

- it includes information about misconduct, or information about misconduct which includes or is accompanied by a Personal Work-Related Grievance;
- Hostplus has breached employment or other laws punishable by imprisonment for a period of 12 months or more, engaged in conduct that represents a danger to the public, or the disclosure relates to information that suggests misconduct beyond the discloser's personal circumstances;
- the discloser suffers from or is threatened with detriment for making a disclosure; or
- the discloser seeks legal advice or legal representation about the operation of whistleblower protection legislation.

Legal advice should be sought for specific information on employment or contractual law rights. Disclosures that are not about matters covered by this Policy do not qualify for protection under the Whistleblower Laws.

10. Who can receive a report?

10.1. Hostplus' Internal Eligible Recipients

The following people can be contacted to make a whistleblower report:

- The Chief People Officer ("**CPO**");
- The Chief Risk Officer ("**CRO**");
- Any other Officer (including a Director, Company Secretary or member of the Hostplus Executive Leadership Team) of Hostplus;
- A Director of the Trustee;
- An auditor, including a member of an audit team conducting an audit, of Hostplus; or
- An actuary of Hostplus.

Alternatively, Hostplus has engaged an independent organisation to provide a confidential, secure and 24/7/365 service where a whistleblower can make a disclosure by:

- placing a free call to the Whistleblower Hotline on 1300 656 894;
- forwarding a complaint/disclosure to a confidential email address (hostplus@myvault.net.au); or
- forwarding a complaint/disclosure to a confidential postal address (HOSTPLUS, C/- Fraud & Forensic Consulting, GPO Box 4736, Melbourne VIC 3001).

Reports received by the Whistleblower Hotline service will be forwarded to Hostplus within 48 hours of the alleged misconduct being reported. The CRO is responsible for receiving and actioning these reports. A whistleblower can also receive updates on the status of their disclosure, and provide additional information where requested, while retaining anonymity.

Where appropriate, whistleblowers are encouraged to make use of one of Hostplus' Internal Eligible Recipients in the first instance. This enables Hostplus to act quickly to identify and address wrongdoing as early as possible.

10.2. External Eligible Recipients

In addition to the above, a report can also be made to one of the following External Eligible Recipients:

- An external auditor of Hostplus, including a member of an audit team conducting an audit; or
- a registered tax agent or BAS agent which provides services to Hostplus (in relation to the tax affairs of Hostplus or an associate of Hostplus).

10.3. Other External Parties and Regulatory Bodies

A report can also be made to:

- Australian Securities and Investment Commission ("ASIC"). For more information on how ASIC handles whistleblower reports, refer to ASIC Information Sheet 239.
- Australian Prudential Regulation Authority ("APRA"). For more information, refer to https://www.apra.gov.au/become-a-whistleblower-or-make-a-public-interest-disclosure
- The Australian Federal Police ("AFP").
- The Australian Tax Office ("ATO") or the Commissioner of Taxation. These disclosures must be in relation to information about tax avoidance behaviour and other tax issues. For more information, refer to https://www.ato.gov.au/general/gen/whistleblowers/.
- A legal practitioner who is consulted for the purpose of obtaining legal advice or legal representation relating to a disclosure. In this instance, the disclosure will be protected even where the legal practitioner concludes that a disclosure does not relate to a Disclosable Matter (as set out in section 7).

Under very limited circumstances protected reports can be made to other recipients (**journalists** and **members of the Commonwealth, state or territory parliament**) through a Public Interest Disclosure or Emergency Disclosure. A disclosure of information qualifies for protection as a Public Interest Disclosure or Emergency Disclosure if:

- the discloser has previously made a disclosure of that information (a previous disclosure) to ASIC, APRA or other applicable Commonwealth entity and this previous disclosure qualifies for protection under section 1317AA(1) of the Corporations Act;
- the discloser does not have Reasonable Grounds to believe that any action is being, or has been, taken to address the matters to which the previous disclosure related;
- For a Public Interest Disclosure: At least 90 days have passed since the previous disclosure was made and the discloser has Reasonable Grounds to believe that making a further disclosure of the information is in the public interest;
- For a Public Interest Disclosure: After at least 90 days have passed since the previous disclosure was made and before making the Public Interest Disclosure, the discloser gives written notice to the body to which the previous disclosure was made that includes sufficient information to identify the previous disclosure and states that the discloser intends to make a Public Interest Disclosure;
- For an Emergency Disclosure: The discloser has reasonable grounds to believe that the information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment. The extent of the information disclosed must be no greater than is necessary to inform the recipient of the substantial and imminent danger; and
- For an Emergency Disclosure: Before making the Emergency Disclosure, the discloser gives written notice to the body to which the previous disclosure was made that includes sufficient information to identify the previous disclosure and states that the discloser intends to make an Emergency Disclosure.

Hostplus staff are encouraged to visit the ASIC website (www.asic.gov.au) to further understand the requirements to make such a report and to seek independent legal advice before making a Public Interest disclosure or emergency disclosure.

A whistleblower may make a report directly to the external parties and regulatory bodies above, about a Disclosable Matter and qualify for protection under this Policy and the law, without making a prior disclosure to Hostplus.

11. Anonymous reporting

Disclosures can be made anonymously or a pseudonym may be adopted by the discloser. There is no requirement for a whistleblower to give their name, both when making the report and at any point during follow-up interactions. A whistleblower can refuse to answer questions that they feel could reveal their identity.

Where possible, whistleblowers that wish to remain anonymous should maintain ongoing two-way communication to support the investigation and to be provided with updates. Without this, the extent of the investigation that can be performed may be limited. Where possible, Hostplus will communicate with the discloser through the anonymous Whistleblower Hotline or through anonymised email addresses.

If a report is made by email and the person's identity cannot be determined from the email address or the discloser does not identify themselves in the email, it will be treated as an anonymous disclosure.

Anonymous reports will still receive the whistleblower protections under the Corporations Act.

12. Identity protection (confidentiality)

Hostplus will protect the confidentiality of a discloser's identity wherever possible, no matter which Internal Eligible Recipient receives the report. Care will be taken during investigation of the report to only share as much information as is reasonably necessary to substantiate the claims made by the whistleblower. This includes taking the following steps:

- all personal information or reference to the discloser 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 selected and qualified staff.

It is illegal for an Eligible Recipient to disclose the identity of the whistleblower or information that is likely to lead to the identification of the whistleblower, where this confidential information was obtained directly or indirectly because the person made a disclosure that qualifies for protection (except in very limited circumstances, set out below). However, in practice, in circumstances some people may be able to guess the discloser's identity. For example, if the discloser has previously mentioned the events at hand to other people, or where the discloser is one of only a small number of people who could have been privy to the information.

Eligible Recipients may disclose information contained in the disclosure (without consent) if:

- the information does not include the discloser's identity;
- Hostplus has taken all reasonable steps to reduce the risk that the discloser will be identified from the information; and
- it is reasonably necessary for investigating the issues raised in the disclosure.

Hostplus may only disclose the identity of the whistleblower in very limited circumstances. These include:

- to ASIC, APRA, or a member of the AFP;
- to a legal practitioner (for the purposes of obtaining legal advice or legal representation about the whistleblower provisions in the Corporations Act or the Taxation Administration Act); or
- with the consent of the discloser.

If a whistleblower is unhappy with the treatment of their report in relation to confidentiality, they may make a report to the Hostplus Privacy Officer or with a regulator, such as ASIC, APRA or the ATO, for further investigation.

Information and data received under this Policy are also covered by the Hostplus Privacy Policy.

13. Legal protections and support available to whistleblowers

Hostplus does not tolerate any form of victimisation or retaliatory action against people who raise concerns with Hostplus. Whistleblowers who make a report about a Disclosable Matter and to an Eligible Recipient, are protected under the law. Whistleblowers that meet the criteria of this Policy and who make a report on a Disclosable Matter will be provided legal protections. These include:

- Protection from any civil, criminal or administrative liability, including any disciplinary action;
- Protection from any victimisation, including threats, harassment, injury or any other negative impacts as a result of making the disclosure;
- Any information that is part of a disclosure is not admissible in evidence against a whistleblower in (if any) criminal proceedings or proceedings involving a penalty, except in proceedings about the falsification of the information;
- Prohibition against the breaking of any contract that is in place with the discloser due to them revealing the information in the disclosure; and
- Prohibition against employment termination on the basis of the disclosure.

Protections apply not only to internal disclosures, but to disclosures to legal practitioners, regulatory and other external bodies, and Public Interest Disclosures and Emergency Disclosures that are made in accordance with the Corporations Act.

13.1. Protection from victimisation

A whistleblower has protection from victimisation. Victimisation is where a person engages in conduct that causes detriment to a discloser, 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 that belief or suspicion is or forms part of the reasons for the victimising conduct. No employee, officer or contractor of Hostplus may engage in detrimental conduct against a discloser who has made or proposes to make a report in accordance with this Policy.

Victimising conduct also includes threats (express or implied, conditional, or unconditional) to cause detriment.

"Detriment" may come in many forms and includes (but is not limited to):

- dismissal of an employee;
- injury of an employee in his or her employment;
- alteration of an employee's position or duties to his or her disadvantage;
- discrimination between an employee and other employees of the same employer;

- harassment or intimidation of a person;
- harm or injury to a person, including psychological harm;
- damage to a person's property;
- damage to a person's reputation;
- damage to a person's business or financial position; or
- any other damage to a person.

All reasonable steps will be taken to ensure that a whistleblower will not be subject to any form of detriment or victimisation, including discrimination, injury, damage, harassment, demotion, dismissal or prejudice, because they have made a report.

Actions that will not be deemed as detrimental conduct under this Policy include:

- Administrative action that is reasonable to protect 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); or
- Managing a discloser's unsatisfactory work performance in line with Hostplus performance management protocols.

Hostplus considers victimisation to be misconduct and takes any behaviour of this kind seriously. If a person feels that they have been victimised because of concerns that they have raised, or if a person becomes aware that someone else has been victimised because of concerns that they have raised, a report should be made immediately to Hostplus' PP&C team. 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.

Hostplus will ensure the discloser understands the reasons for any administrative or management actions taken.

There are steep penalties and the potential for criminal prosecution for those who engage in victimising conduct.

13.2. Compensation and remedies

A whistleblower may seek compensation or remedy through the courts if they suffer loss, damage or injury because of a disclosure and Hostplus failed to take reasonable precautions and exercise due diligence to prevent this detriment. In this instance, a whistleblower should seek independent legal advice.

Hostplus will also provide the discloser support, including:

- access to the Hostplus Employee Assistance Program ("EAP");
- access to an independent support person from the PP&C Team, if requested; and
- regular updates during the investigation (where possible).

13.3. Civil, criminal and administrative liability protection

Disclosers are protected from the following in relation to their disclosure:

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

No contractual or other remedy may be enforced, or contractual right exercised, against a whistleblower based on the disclosure. However, a whistleblower may be liable for any misconduct

that they have engaged in that is revealed by their disclosure (or revealed by an investigation following their disclosure).

If the report is made to ASIC, APRA, or the Commissioner of Taxation (or other prescribed regulators) or is a Public Interest Disclosure or Emergency Disclosure, the information contained in the report cannot be admissible in evidence against the person in criminal proceedings or in proceedings of a penalty other than proceedings concerning the falsity of the information.

14. Investigating a report

Where a report is made under this Policy, the CRO will undertake an investigation. Hostplus will need to assess each disclosure to determine whether it qualifies for protection and whether a formal, in-depth investigation is required. Hostplus is committed to all investigations being undertaken in an objective, fair and independent manner.

Hostplus will acknowledge receipt of a report, by notifying the discloser (upon receipt). In undertaking this investigation, the CRO (or other nominated person) will:

- consider who (internal or external) should lead the investigation – including whether an independent party is required to investigate the matter, including reporting directly to the Board and/or Audit Committee and Risk and Compliance Committee (where relevant). This may be suitable:
    - where additional skills or expertise would be advantageous; or
    - where the matter relates to fraud or corruption, to ensure that the investigation also aligns with the Fraud and Corruption Policy investigation procedures.
- ensure each person who is involved in handling and investigating the disclosure understands the confidentiality requirements, including that an unauthorised disclosure of a discloser's identity may be a criminal offence;
- determine the nature and scope of the investigation;
- determine any technical, financial or legal advice that may be required to support the investigation;
- commit to a timeframe for the investigation;
- set parameters for regular updates to be provided to the whistleblower (where possible);
- consider when it is appropriate to inform an individual who is the subject of the investigation. In making this decision, the investigation leader will consider when it is appropriate to enable procedural fairness but also to protect the integrity of the investigation (that is, to prevent information from being destroyed or to allow time for regulators or law enforcement to be notified);
- consider whether any actions are immediately required to protect the discloser from a risk of detriment. These may include allowing the whistleblower to perform their duties from another location or reassigning them to another role at the same level;
- consider whether any strategies are required to minimise and manage stress, time or performance impacts of the investigation on the whistleblower. This must include referral to the EAP and a PP&C support person (as outlined in section 13.2);

- undertake the investigation. Hostplus will aim to conclude the investigations within 30 business days of notification, but that time may vary depending on the nature of the disclosure. More complex matters may take longer to investigate; and
- remind the whistleblower of their rights to lodge a complaint if they have suffered detriment.

Evidence, notes and documents pertaining to the investigation will be stored on a secure share drive, with access restricted to the CRO and any nominated individuals involved in the investigation. Where possible, paper documents will be securely destroyed. Communications and documents relating to the disclosure will not be sent to an email address or printer that can be accessed by other staff.

Where a report is made about the CRO, the Chief People Officer will undertake an investigation and all references above to the role and responsibilities of the CRO in this section should be replaced with the Chief People Officer.

15. Communication of outcome

Where the whistleblower can be contacted, the whistleblower will be provided with regular updates (including through anonymous channels). At a minimum, this must include an update on when the investigation begins, when the investigation is in progress and after the investigation has been finalised. However, there may be circumstances where it is not appropriate to provide the outcome of the report to the discloser.

The findings from the investigation will also be provided to the Board and/or Audit Committee and Risk and Compliance Committee. This will include the subject matter of the disclosure, the status of the investigation, the action taken for each disclosure, the timeframe for finalising the disclosure, and how the disclosure was finalised.

If a whistleblower is unhappy with the outcome or the investigation process undertaken, they may lodge a complaint with a regulator such as ASIC, APRA or the ATO.

16. Fair treatment of those subject to a disclosure

Hostplus is committed to ensuring the fair treatment of employees who are mentioned in disclosures. No action will be taken against employees or officers who are implicated in a report under this Policy until an investigation has determined whether any allegations against them are substantiated. Where an investigation is warranted, the process will be objective, fair and independent.

Any disclosures that implicate or mention an employee or officer will be kept confidential and must only be disclosed to persons on a need to know basis for proper performance of their functions under this Policy, and for the proper investigation of the report.

An employee or officer who is implicated in a disclosure has a right to be informed of the allegations and must be given an opportunity to respond.

Hostplus will also provide any persons implicated:

- access to the Hostplus Employee Assistance Program ("**EAP**"); and
- access to an independent support person from the PP&C team, if requested.

17. Education and awareness

To ensure that staff are cognisant of the Hostplus whistleblowing mechanism, training is provided during the onboarding process. Additionally, refresher training and education is provided to all staff, with specialist training provided to key individuals with specific responsibilities under this Policy, including the Whistleblower Officer and other Eligible Recipients, as required.

All staff have access to this Policy via the Hostplus intranet, as well as information posters disbursed throughout all common areas in the workplace.

Information relating to this Policy that is relevant to an external audience will be included on Hostplus' website.

For more confidential information about the application of this Policy or related procedures or the protections for whistleblowers under law, please contact the:

- CRO (Whistleblower Officer); and/or
- Whistleblower Hotline (for contact details, refer to section 10.1).

18. Monitoring the effectiveness of the Policy

The Hostplus CRO will provide regular reporting to the Board and/or the Audit Committee and Risk and Compliance Committee on the effectiveness of this Policy and its related processes, while preserving confidentiality. This will include:

- the number and nature of disclosures made in the last quarter (for example, by who, who to and matter type);
- how disclosures were made;
- the status of any investigations underway;
- any actions taken in relation to a disclosure;
- the frequency of communications with disclosers;
- the outcomes of completed investigations; and
- the timeframes for responding to and investigating disclosures.

From time to time, Hostplus may initiate an internal or external audit review, or an internal monitoring review, over the effectiveness of the Policy.

19. Roles and responsibilities

Key roles and responsibilities relating to this Policy are summarised below.

Role	Description of responsibilities
Board of Directors	The Board is responsible for approving the Whistleblowing Policy.
Audit Committee ("**AC**")	The AC is responsible for: • receiving whistleblower reports from the CRO and findings from a whistleblower investigation; • providing objective, non-executive oversight and review of Hostplus' compliance with this Policy; and • overseeing the maintenance of this Policy and maintaining the confidentiality of any related disclosures.

Role	Description of responsibilities

Policy Owner and Whistleblower Officer – Chief Risk Officer ("**CRO**")	The Policy Owner is responsible for:
	• developing and monitoring the implementation of this Policy;
	• periodically reviewing and updating this Policy and associated processes and procedures;
	• regularly reporting to the Board and/or the Audit Committee on the effectiveness of this Policy; and
	• implementing compulsory education and training programs for all employees regarding this Policy and Hostplus' whistleblower program.
	• The Whistleblower Officer is responsible for:
	  ○ receiving and actioning whistleblower reports;
	  ○ undertaking an investigation of a whistleblower report;
	  ○ conducting an assessment of all new disclosures to determine that the disclosure qualifies for protection under this Policy;
	  ○ taking all necessary steps to protect the identity of any Eligible Whistleblower throughout and after the investigation of a disclosure;
	  ○ addressing any concerns raised by an Eligible Whistleblower about the investigation of their disclosure (including breach of confidentiality);
	  ○ solely holding access to a secure share drive which stores evidence, notes and documents pertaining to an investigation of a whistleblower report; and
	  ○ safeguarding disclosers and ensuring the integrity of the reporting mechanism.

Eligible Recipients	The Eligible Recipient is responsible for: • receiving disclosures of Disclosable Matters from Eligible Whistleblowers and treating all such matters as confidential; and • completing compulsory training organised by Hostplus on its processes and procedures for receiving and handling disclosures made under this Policy.
Employees	All Hostplus employees are responsible for: • upon becoming aware of a potential Disclosable Matter, reporting the matter in accordance with this Policy; • upon becoming aware of the identity of a person who has made a whistleblower disclosure, not disclosing (whether directly or indirectly) the identity or any identifying information to anyone else; • not engaging in any detrimental conduct in relation to an Eligible Whistleblower; and • undertaking compulsory education and training programs in relation to Hostplus' whistleblower process and this Policy.

20. Policy review

This Policy is required to be reviewed by the Board, at a minimum, once every two years.

Non-material changes to this Policy may be made with the approval of the Policy Owner. These changes must be notified to the relevant approving Committee or Board and documented in document control information, however, formal approval is not required. Non material changes include:

- minor wording, numbering or grammatical changes for clarity/syntax;
- changes in role titles to reflect organisational changes;
- changes to Committee names; and
- changes to Policy names.