INFOMEDIA™

Global leaders in parts and service software

WHISTLEBLOWER POLICY

1 August 2018

Revised: 1 December 2019

APPLICATION OF THIS POLICY

What is this policy about?

This Policy sets a framework for the reporting of 'Misconduct' as defined in section 4.

Refer to section 4 for the definition of 'Misconduct'.

How is this policy made available?

This policy will be made available via the Company's intranet pages. A copy may be requested at any time from the Company Secretary, General Counsel or Head of People & Culture.

Refer section 1 – 'Introduction'

Who can report & what to report?

Eligible 'Whistleblowers' are entitled to report any behaviour or conduct which implicates Infomedia Ltd, its officers or employees if it amounts to 'Misconduct'.

Refer to section 5 for more detail.

How to report?

If you qualify as a 'Whistleblower', you can make a report verbally or in writing.

Refer to section 6 for more detail.

Who to report to?

Refer to section 7 for detail.

What is the procedure of an Investigation?

Reports of Misconduct are treated seriously and will be assessed to determine whether: (a) they fall within this Policy; (b) if so, whether an Investigation is required. Such investigations shall be coordinated by the appointed 'Whistleblower Investigations Officer'.

Refer to section 4 for the definition of 'WIO' and section 8 for more detail.

What is the outcome of an Investigation?

At the end of the Investigation, the Whistleblower Protection Officer will report their findings to the CEO (where appropriate) who will determine the appropriate response.

Refer to section 9 for more detail.

How are Whistleblowers protected?

If you qualify as a 'Whistleblower', you will be entitled to the protections in section 10.

Refer to section 10 for more detail.

What are the obligations of a Whistleblower?

Exercising your right to act as a 'Whistleblower' comes with serious responsibilities. For example, Whistleblowers need to have reasonable grounds to suspect Misconduct before making a report. Reports that are deliberately false or which are made without reasonable grounds for suspecting Misconduct, may result in disciplinary action.

Refer to section 12 for more detail.

WHISTLEBLOWER POLICY

1. INTRODUCTION

Infomedia is committed to the highest standards of conduct and ethical behaviour in our business activities. The Board of Directors and Executive Leadership Team recognises that any genuine commitment to detecting and preventing illegal, fraudulent, unethical or other undesirable conduct must include a mechanism whereby employees and others can report their concerns freely and without fear of victimisation.

There are protections available under this Policy and at law provided:

a. the person who makes a disclosure is a Whistleblower as defined in section 4 of this Policy;

b. the Whistleblower has reasonable grounds for his/her concern;

c. the concern relates to the types of matters set out at paragraph 4 of this policy under the heading Misconduct; and

d. the Whistleblower raises his/her concern with one of the Eligible Recipients set out at paragraph 4, or as set out at paragraph 7 of this Policy.

This policy will be available on the Company's intranet located at intranet.infomedia.com.au. Alternatively, a hard or soft copy can be made available by request to the Company Secretary, the General Counsel or the Head of People & Culture. A copy will also be made available on the Company's website.

2. OBJECTIVE

The objective of this policy is to:

a. Promote an open and transparent culture within Infomedia.

b. Encourage eligible 'Whistleblowers' (refer definition in section 4 below) to report an issue if they have reasonable grounds to believe a person or persons has engaged in Misconduct.

c. Demonstrate Infomedia's commitment to a fair workplace and outline the process for reporting and managing reports of Misconduct.

d. Protect individuals who report Misconduct in line with this policy and which they reasonably believe to be corrupt, illegal or unethical on a confidential basis, without fear of Victimisation, including dismissal or discriminatory treatment.

e. Ensure that matters of Misconduct are identified and addressed appropriately.

3. COMMENCEMENT & SCOPE

This policy commences with effect from 1 December 2019.

This Policy applies to Infomedia and all of Infomedia's current and former:

a. Officers and employees;

b. Consultants, secondees and volunteers;

c. Associates (such directors and company secretaries of related companies within Infomedia); and

d. Contractors, suppliers, agents and their employees.

Where local laws apply, they will supplement and prevail over this Policy to the extent required by law, or where the Company has agreed in its contractual arrangements with third parties.

This policy should not be used for complaints relating to personal work-related grievances, such as an interpersonal conflict between the discloser and another person, a decision relating to engagement, transfer or promotion of the discloser, a decision relating to the terms and conditions of engagement of the discloser, or a decision relating to suspension, termination or discipline of the discloser. Concerns of that nature should be raised with the Head of People & Culture.

This policy is not intended to replace other reporting structures or grievance procedures and should be read in context with other policies.

This Policy is not intended to be contractually binding and does not form part of any contract the Whistleblower may have with Infomedia.

4. DEFINITIONS

For the purposes of this Policy, certain words are defined as follows:

APRA means the Australian Prudential Regulatory Authority.

ASIC means the Australian Securities and Investments Commission.

Detriment means dismissal, demotion, intimidation, physical or psychological harm, harassment, discrimination, disciplinary action, bias, threats, damage to property, damage to

reputation, any other damage to a person or other unfavourable treatment. **Detriment** does not include reasonable management action to protect a person from detriment (for example reallocating duties or reporting lines) or to manage unsatisfactory performance of a person who is or may be a Whistleblower.

Infomedia is a reference to Infomedia Ltd ACN 003 326 243 and its related bodies corporate.

Investigation: means a search and review of evidence (actual and circumstantial) connecting or tending to connect a person (either a natural person or a body corporate) with conduct that infringes the policies and standards set by Infomedia.

Eligible Recipient means in relation to Infomedia, any officer, director or senior manager, auditor (including any member of the audit team conducting an audit) or any other person authorised to receive disclosures under this Policy (eg the WPO) or by law. If the disclosure relates to Infomedia's tax affairs, the Whistleblower may also make a report to a director, company secretary or senior manager within Infomedia; a member of Infomedia's tax team and a registered tax agent of Infomedia.

The 'senior managers' of Infomedia are the CEO and those parties reporting directly to the CEO: at the time of publication this means:

- Chief Executive Officer
- Chief Financial Officer
- Head of People & Culture
- Chief Operations Officer
- Chief Technology Officer
- General Counsel
- Company Secretary
- Any CEO or Head of Region (APAC, Americas or EMEA)
- Any VP of Product or business division

Eligible Whistleblower means any current or former Infomedia employee, officer, director, contractor (including by extension, employees of the contractor) and associates of Infomedia. It also includes relatives and dependants of those parties, and any other party specified as an 'eligible whistleblower' by the Corporations Act 2001 (Cth).

Misconduct: means any of the following types of behaviours or conduct in respect of Infomedia:

- Fraud, negligence, default, breach of trust and breach of duty.
- An improper state of affairs or circumstances, including the matters listed below:
    - Information that indicates that Infomedia or any of its officers or employees have engaged in conduct that constitutes a breach of the Corporations Act or other laws administered by ASIC and APRA.

- Information that indicates that Infomedia or any of its officers or employees have engaged in conduct that breaches any other *Commonwealth laws punishable by 12 months or more imprisonment*
- Misleading or deceptive conduct, including conduct or representations which amount to improper or misleading accounting or financial reporting practices.
- A breach o Infomedia policies or Code of Conduct, including any failure to properly apply this Policy.
- Conduct within Infomedia's control which is a significant danger to the environment.
- Conduct endangering the health and safety of any person or persons which has been reported to management but not acted upon.
- Conduct which represents a danger to the public or the financial system.
- Substantial wasting of resources or other acts causing financial loss to Infomedia, damage to its reputation or its interests generally.
- Any action taken against, or harm suffered by a person as a result of making a report under this Policy.
- Any attempt to conceal or delay disclosure of any of the above conduct

However; Misconduct **<u>does not</u>** include conduct which:

- concerns a personal work-related grievance of the discloser.
- does not concern detriment caused to the discloser or a threat made to the discloser.

Victimisation includes conduct that causes Detriment to another person or constitutes the making of a threat to cause Detriment to another person, where the reason (or part of the reason) for that conduct is a belief or suspicion that the other person (or any other person) made, may have made, proposes to make, or could make a disclosure under this Policy.

Whistleblower: means any Eligible Whistleblower who makes, attempts to make or wishes to make a report in connection with Misconduct and where the Whistleblower wishes to avail themselves of protection against reprisal for having made the report under this Policy and/or applicable legislation.

Whistleblower Protection Officer (WPO): means the designated Infomedia representative tasked with the responsibility of protecting and safeguarding the interests of Whistleblowers within the meaning of this Policy. The WPO will have access to independent financial, legal and operational advisers as required. The WPO is Infomedia's General Counsel. If the General Counsel is implicated in the allegation of Misconduct, or is otherwise cannot act due to a conflict of interest, the Company acting through its directors or CEO (as may be appropriate)

may appoint a temporary WPO for a period of time or in relation to a specific matter and any resulting Investigation.

Whistleblower Investigations Officer (WIO): means the designated Infomedia representative tasked with the responsibility of conducting preliminary investigations into reports received from a Whistleblower. The role of the WIO is to investigate the substance of the complaint to determine whether there is evidence in support of the matters raised or, alternatively, to refute the report made. The WIO will be appointed by the WPO on a case by case basis, depending on the nature of the report. The WIO will be independent from the area under investigation. The WIO may be a manager once removed from the Whistleblower if they are not implicated in the allegation of Misconduct. Other resources within the group or externally can be engaged to assist in the investigation as deemed necessary by the WIO and/or the WPO.

5. WHO CAN REPORT & WHAT TO REPORT

Eligible Whistleblowers are encouraged to report any information which they reasonably believe implicates any Infomedia, or any officer or employee of those entities in any act or omission amounting to Misconduct.

6. HOW TO REPORT

Verbally

Whistleblowers may report Misconduct verbally. Where a verbal report is made in accordance with this Policy, the Whistleblower may be requested to provide further documentation in support of the alleged conduct, including for instance, a completed Misconduct Report Form.

In writing

Whistleblowers may report Misconduct in writing via the channels outlined in section 7 below. The Misconduct Report Form (refer Schedule 1) is the preferred method by which a report should be filed.

7. WHO TO REPORT TO

Internal Reporting

Whistleblowers are encouraged to make internal reports to any of the Eligible Recipients listed in section 4 of this Policy, preferably to the WPO.

All reports made under this Policy will be treated seriously and will be dealt with in accordance with the processes outlined in this document.

Reporting Misconduct to third parties outside the Company

It is the Company's preference that eligible Whistleblowers do not discuss internal matters with external parties. The Company's policies (including this policy) provide appropriate internal mechanisms to raise Misconduct.

However, nothing in this Policy should be interpreted as restricting a Whistleblower from reporting Misconduct to an external party, if that is required or permitted by any relevant law or regulation.

Whistleblowers may make disclosures to ASIC, the Company's external auditors or any other recipient prescribed by law. A Whistleblower intending to report outside the Company should take reasonable steps to apprise themselves of the law as it applies to such disclosures.

8. INVESTIGATION OF MISCONDUCT REPORTS

All reports of Misconduct will be treated seriously and assessed to determine whether: (a) they fall within this Policy; and (b) if so, an Investigation is required. Investigations are to be undertaken by the WIO. The WIO responds to all concerns raised and reports to the WPO.

Procedure of the Investigation

Following a report of Misconduct, either internally or externally, the following procedure will be followed:

1. The Eligible Recipient is to complete a Misconduct Report Form (**MRF**) and confidentially forward it to the WPO. The identity of the Whistleblower will be kept confidential, except in the limited circumstances permitted by the law (see paragraph **Error! Reference source not found.** titled 'Protection of Whistleblowers below)
2. The WPO selects an appropriate WIO.
3. The MRF is confidentially forwarded to the WIO by the WPO.
4. The WIO reviews the MRF, determines the substance of the allegations and forms a recommendation as to the appropriate manner of investigation (if any).
5. The WIO recommends to the WPO whether an investigation should proceed, and if so, how that investigation might proceed. The WPO then informs the Whistleblower.
6. The WIO determines necessary resources and secures access to those resources, including where necessary, other employees or external professional help (including lawyers, accountants, forensic analysts or operational experts).
7. The WIO conducts an investigation to gather relevant facts and evidence under the guidance of the General Counsel or such other appointed legal advisors. This may include speaking with the Whistleblower (if possible) and interviewing witnesses.
8. The WIO to consider process/control improvements (risk assessments, audits, etc.).

9. The WIO prepares and presents the evidence to the General Counsel and a report will be prepared under the direction of the General Counsel.
10. The final Investigation Report is shared with the CEO and/or the Directors as appropriate and remedial actions (if any) applied in line with section 9 below.
11. The WPO advises and debriefs the Whistleblower. A copy of the Investigation report will not be made available due to matters of privacy, confidentiality and/or legal privilege.

Conduct of the Investigation

The WIO will conduct an evidence-based Investigation consistent with the requirements outlined in this Policy. Infomedia will take reasonable steps to ensure that the Investigation is conducted in an un-biased and timely manner.

Infomedia's usual practice is to ensure that any investigation process is confidential and fair. Where appropriate and subject to our requirements to maintain confidentiality, accused parties shall be entitled to a right of reply to the WIO and to put evidence in support of their position as part of the investigation. Accused parties must submit their evidence in a timely manner and in this regard the Company may set reasonable timelines by which evidence is to be submitted.

Infomedia will endeavour to maintain the privacy of employees who are mentioned in a disclosure or to who a disclosure relates.

Employees who are mentioned in a disclosure are entitled to support services such as Infomedia's Employee Assistance Program.

Fair treatment of employees mentioned in disclosures

Infomedia's usual practice is to ensure that any investigation process is confidential and fair. Infomedia will endeavour to maintain the privacy of employees who are mentioned in a disclosure or to who a disclosure relates.

9. REPORTING OF INVESTIGATION FINDINGS

At the end of the investigation, the WPO will report their findings to the CEO who will determine the appropriate response. If the CEO is involved, or where otherwise deemed appropriate, this response will include addressing any unacceptable conduct and taking remedial action required to prevent any future occurrences of the same Misconduct.

All reported incidents and investigation outcomes will be reported to the Audit & Risk Committee.

Disciplinary action arising from a finding of Misconduct shall be in line with the Infomedia Performance Management and Disciplinary Policy and Procedure. If the CEO or a member of the Board is the subject of an allegation of Misconduct, the Chairman of the Audit & Risk Committee will determine corrective measures.

Where allegations of Misconduct made against another person have been Investigated but cannot be substantiated, that reported person will be advised accordingly that the reported matter was investigated, no case was found to be answered and no further action will be taken.

10. PROTECTION OF WHISTLEBLOWERS

If a person makes a disclosure that qualifies for protection under the relevant Whistleblower protections, then the following shall apply:

Protection of identity / anonymity

The identity of the Whistleblower must be kept confidential by the Eligible Recipient who first receives a disclosure from the Whistleblower unless:

- the Whistleblower consents to the disclosure; or
- Infomedia needs to disclose this information to obtain confidential legal advice or representation; or
- the disclosure is authorised or required by law. This may include for example (without limitation) disclosures made to the ASIC, APRA or the Australian Federal Police; or
- During the investigation process, Infomedia is permitted to disclose information (other than the identity of the discloser) reasonably necessary for the purposes of investigating the disclosure. Infomedia will take reasonable steps to reduce the risk of the discloser being identified.

This protection extends to include disclosures about the identity of the Whistleblower or information which is likely to lead to the identification of the Whistleblower.

If you receive information about the identity of a Whistleblower (whether directly or indirectly), you must keep that information confidential (except in the circumstances permitted above). If you do not keep that information confidential or you disclose information likely to lead to the Whistleblower being identified (except in the circumstances permitted above) then:

- if you are an employee or officer of Infomedia– you will be subject to disciplinary action, which may include a formal written warning, or dismissal,
- if you are a contractor, supplier etc – Infomedia may terminate your engagement or appointment, or take other appropriate corrective action; and
- you may be exposed to criminal and civil penalties, including substantial fines and / or jail.

Protection from Victimisation

A Whistleblower who reports Misconduct in accordance with this Policy must not be Victimised. Infomedia will not tolerate a Whistleblower being Victimised

A Whistleblower who believes he or she has been Victimised, should immediately report the matter to the WPO.

Any Infomedia employee, director, contractor, partner, supplier or consultant who is found to have Victimised a Whistleblower in contravention of this Policy:

- will be subject to disciplinary or other corrective action by Infomedia, including dismissal from employment or termination of contract; and
- may be exposed to civil and criminal penalties.

Protection of files and records

All information, documents, records and reports relating to the investigation of reported Misconduct will be confidentially stored and retained in an appropriate and secure manner by the WPO and subject to legal privilege. Unauthorised release of information to someone not involved in the investigation (other than senior managers or directors who need to know to take appropriate action, or for corporate governance or legal purposes) will be a breach of this Policy and will be dealt with under Infomedia disciplinary procedures.

Support and protections provided by Infomedia to Whistleblowers

If the Whistleblower is an Infomedia employee or officer, they are entitled to support through the Employee Assistance Program. Infomedia may explore other options on a case by case basis.

The Whistleblower will not be subject to disciplinary action for reporting Misconduct in accordance with this Policy. The Whistleblower may however still be subject to disciplinary action for any involvement which they had in the Misconduct. Infomedia may take the disclosure into account when determining the nature of any disciplinary action taken against the Whistleblower in that event.

If the Whistleblower thinks his/her disclosure has not been dealt with sufficiently, he/she may raise the concern with the CEO , if they have not already done so, or report this concern under this Policy.

Legal Protections

There are protections under applicable Whistleblower laws for those making a report under this Policy, including protection from legal action for making a disclosure. This does not include protection from any legal action for illegal or improper conduct the Whistleblower may have engaged in that is revealed as a result of his/her report.

11. FEEDBACK

Where possible, and assuming the identity of the Whistleblower is known, the Whistleblower will be kept informed of the outcome of the investigation of his or her report, subject to privacy, confidentiality and legal considerations. All Whistleblowers must maintain confidentiality of all such reports and not disclose details to any person.

12. FALSE REPORTS OR ABSENCE OF REASONABLE GROUNDS FOR SUSPICION

Whilst not intending to discourage Whistleblowers from reporting matters of genuine concern, Whistleblowers must ensure as far as possible, that reports of Misconduct are based on a reasonable suspicion that Misconduct has occurred. Reports should be factually accurate, complete, based on firsthand knowledge (not hearsay) and without material omission.

Where it is established by the WIO that the report is deliberately false or that there was no reasonable basis for suspecting the Misconduct referred to in the report, then the Whistleblower may be subject to disciplinary proceedings up to and including dismissal.

The protections for Whistleblowers referred to in this Policy and at law are not available if a disclosure is made without reasonable grounds and is deliberately false. Deliberate false reports involve a Whistleblower reporting information they know to be untrue. It does not include situations where the Whistleblower reasonably suspects misconduct, but their suspicions are later determined to be unfounded.

13. POLICY REVIEW

Infomedia's Whistleblower Policy will be reviewed periodically by the Audit & Risk Committee. A report will be made to the Board of the outcome of each review and any recommended changes to the Policy.

Misconduct Report Form

The purpose of this form is to facilitate the report of allegations of 'Misconduct' under Infomedia's Whistleblower Policy. Please provide the following details if you have reasonable grounds to suspect that Misconduct has occurred. Please note that, if possible, you may be called upon to assist in the investigation.

Note: Please follow the guidelines as laid out in the Infomedia Whistleblower Policy when filling out this form.

REPORTER'S CONTACT INFORMATION ***Important note**: To enable Infomedia to properly investigate and respond to your disclosure, we encourage (but do not require) you to provide your name when making the disclosure. If you are comfortable doing so, we will provide your identity to those at Infomedia who are in charge of investigating whistleblower disclosures (Whistleblower Protection Officer and Whistleblower Investigations Officer). We will then be able to easily provide you with information about the status of any investigation into your disclosure. Therefore, we ask you to please provide your written consent to do so.* *If you are not comfortable being identified internally, Infomedia will respect your wishes and maintain confidentiality of your identity. In this scenario, we recommend setting up an anonymised email address to maintain an ongoing two-way communication with Infomedia (eg parties asking follow-up questions or provide feedback). In any case, please note that the person investigating the disclosure may not be able to easily provide you with information about the status of any investigation into the conduct.* *Note that there are certain circumstances permitted by law in which Infomedia is permitted to disclose your identity - these are set out in Infomedia's Whistleblowing Policy. However please note that Infomedia will take all reasonable steps to avoid doing so unless necessary and permitted by the law*	
NAME/ PSEUDONYM	
CONTACT NUMBER	
EMAIL ADDRESS	

Briefly describe the alleged Misconduct below and provide any supporting documentation, if available. If there is more than one allegation of Misconduct, number each allegation and use as many pages as necessary.
1. What is the alleged Misconduct that occurred?
2. When and how did the alleged Misconduct come to your attention?

3. Who was involved in the alleged Misconduct?
4. When did the alleged incident of Misconduct occur?
5. Where did the alleged Misconduct occur?
6. Is there any supporting evidence to substantiate the alleged Misconduct? If so, please describe and annex to this Form (eg documents, emails or the name of any potential witnesses).
7. Do you have any other details or information which may assist us to investigate this matter?
8. Any other comments?

Please read the following statement before signing this form:

Whistleblowers must ensure as far as possible, that reports of Misconduct are based on a reasonable suspicion that Misconduct has occurred. Reports should be factually accurate, complete, based on firsthand knowledge (not hearsay) and without material omission.

Where it is established that the report is deliberately false or that there was no reasonable basis for suspecting the Misconduct referred to in the report, then the Whistleblower may be subject to disciplinary proceedings up to and including dismissal. The protections for Whistleblowers referred to in the Whistleblower Policy, and at law, are not available if a disclosure is made without reasonable grounds and is deliberately false. Please refer to Infomedia's Whistleblowing Policy for guidance.

DATE:	SIGNATURE:

Next Steps: Please submit this Form to an Eligible Recipient, as defined in the Policy. This form will be confidentially forwarded on from the Eligible Recipient to the Whistleblower Protection Officer (**WPO**). The WPO will select an appropriate Whistleblower Investigation Officer (**WIO**) to investigate the alleged Misconduct.