

**ASPEN PHARMACARE HOLDINGS LIMITED
AND IT'S SUBSIDIARIES'
("Aspen", "the Group", "we" or "our")**

WHISTLEBLOWING POLICY

1. BACKGROUND

- 1.1. Aspen is committed to conducting its business according to the highest ethical standards and in accordance with applicable laws.
- 1.2. In line with this commitment, and Aspen's commitment to open communication, this Policy aims to provide an avenue for employees, customers, suppliers and other stakeholders, on an anonymous basis if preferred, to raise concerns regarding improper conduct within Aspen, without fear of retaliation.
- 1.3. This Policy does not form part of any employment contract and may be amended at Aspen's discretion.

2. WHO CAN RAISE CONCERNS OR DISCLOSE IMPROPER CONDUCT

The reporting mechanisms set out in this Policy are available to all employees, suppliers and customers of Aspen, or other eligible stakeholders as prescribed under applicable laws.

3. DISCLOSURES WHICH QUALIFY FOR PROTECTION

- 3.1. A disclosure of information is protected under this Policy if the person has **reasonable grounds** to suspect that the information concerns or indicates **improper conduct** in relation to a Group entity, employee or officer, and the disclosure is made in accordance with this Policy ("**Protected Disclosure**").
- 3.2. Improper conduct includes –
 - 3.2.1. a violation of the Aspen Code of Conduct, or any other policy under which Aspen operates;
 - 3.2.2. a violation of applicable laws; or
 - 3.2.3. conduct that presents a danger to the public or to the environment.
- 3.3. Below are examples of the type of improper conduct that can be reported:

- Fraud;
- Money laundering;
- Discrimination or harassment;
- Violation of competition laws;
- Violation of data privacy laws;
- Conflicts of Interest;
- Bribery / Corruption;
- Violation of an applicable industry code of conduct;
- Environmental, health & safety issues;
- Theft or improper use of company assets / resources;
- Improper:
 - accounting practices,
 - internal accounting controls, financial reporting; or
 - auditing matters;
- Insider trading;
- Unlawful disclosure or misappropriation of Aspen intellectual property or confidential information; or
- Violation of policies and procedures that underpin the Aspen Code of Conduct, including policies on gifts, entertainment and hospitality.

4. DUTIES OF EMPLOYEES IN RELATION TO IMPROPER CONDUCT

Employees of Aspen who become aware of improper conduct are expected to report the matter by making a Protected Disclosure under this Policy.

5. HOW TO GO ABOUT REPORTING IMPROPER CONDUCT

5.1. Internal Reporting

5.1.1. A Protected Disclosure can be raised through any of the following internal channels (the “**Internal Reporting Outlets**”):

5.1.1.1. an immediate supervisor or line manager;

5.1.1.2. the senior executive responsible for your operation, division or area;

5.1.1.3. the Internal Auditors, Company Secretary & Group Governance Officer, the Group Legal Officer & Group Compliance Officer or the in-house Aspen Legal Counsel responsible for supporting the Aspen company by whom you are employed;

5.1.1.4. if you believe that the matter cannot be appropriately dealt with through the channels recorded in **paragraphs 5.1.1.1 to 5.1.1.3** above, or if you are an external party wishing to raise a concern, you can make use of the Tip-offs Anonymous service, as described in **paragraph 6** below; or

- 5.1.1.5. if you believe that the matter has not been investigated or handled appropriately via any of the mechanisms recorded in **paragraphs 5.1.1.1 to 5.1.1.4**, you may contact the Chief Audit Executive as follows: mLorgat@aspenpharma.com.
- 5.1.2. Irrespective of the Internal Reporting Outlet used, to enable Aspen to properly investigate your Protected Disclosure, please provide as much detailed information as possible, including:
 - 5.1.2.1. a description of the suspicion, concern or alleged improper conduct;
 - 5.1.2.2. the names of the implicated persons, their line manager and the names of any witnesses or other parties who may be aware of the matter; and
 - 5.1.2.3. any emails or documents that may support the allegation.

5.2. External and Public Reporting

- 5.2.1. In considering whether to take a concern outside of Aspen, you should consider whether reporting the concern externally, without first giving Aspen the opportunity to look into the matter, is a reasonable course of action. It would not normally be appropriate to disclose your concerns externally unless you have first followed the procedures in this Policy.
- 5.2.2. If however:
 - 5.2.2.1. you have reasonable grounds to believe that, by using one of the Internal Reporting Outlets, the investigation into the alleged improper conduct could be jeopardised; or
 - 5.2.2.2. Aspen has failed to respond to your Protected Disclosure within the maximum period allowed under applicable law; or
 - 5.2.2.3. the Internal Reporting Outlets have been otherwise exhausted,then you can, subject to applicable law, report your concern **externally** to the relevant **competent national authority**.
- 5.2.3. You can only make a **public disclosure** regarding your concern (for example to the press or via social media) as permitted under applicable laws.

6. TIP-OFFS ANONYMOUS

- 6.1. Tip-Offs Anonymous is a confidential reporting service operated by an independent third party contracted to Aspen (the “**Service Provider**”), and is

available 24 hours a day, 365 days a year. The Service Provider can accommodate Protected Disclosures in many languages and can be contacted directly from most locations.

- 6.2. There are five options for submitting a Protected Disclosure via Tip-Offs Anonymous:
- 6.2.1. Online: <https://www.tip-offs.com/MakeReport.aspx>
 - 6.2.2. By email: aspenpharma@tip-offs.com
 - 6.2.3. By post : Tip-offs Anonymous, PO Box 774, Umhlanga Rocks, 4320, Republic of South Africa
 - 6.2.4. By fax: +27 31 5607395
 - 6.2.5. By phone, using the appropriate FreeCall telephone numbers recorded on the Aspen website: <https://www.aspenpharma.com/ethics-management-and-tip-offs/>.

7. WHAT HAPPENS TO A PROTECTED DISCLOSURE

- 7.1. If you make a Protected Disclosure using one of the Internal Reporting Outlets described in **paragraphs 5.1.1.1 to 5.1.1.3** above:
- 7.1.1. Your report will follow the in-country procedure for reporting and investigation, as directed by local management, with escalation to the Group Ethics Committee where considered appropriate;
 - 7.1.2. Aspen shall acknowledge receipt of and provide feedback in respect of your Protected Disclosure within the timelines prescribed under applicable laws; and
 - 7.1.3. Aspen shall designate an impartial person or department for following up on the reports, who will maintain communication with you and, where necessary, ask for further information from and provide feedback to you.
- 7.2. The following steps will be followed if you make a Protected Disclosure using the Internal Reporting Outlet described in **paragraph 5.1.1.4** (Tip-Offs Anonymous):
- 7.2.1. **Step 1:** If the Protected Disclosure is submitted via a live telephone operator or the Tip-Offs Anonymous website, a reference number will be provided which can be used to request feedback on actions taken. If a voice recording service is used, feedback will only be possible if contact details are provided as part of the message submitted.
 - 7.2.2. **Step 2:** The Service Provider will discuss your Protected Disclosure, in order to obtain as much information as possible.

- 7.2.3. **Step 3:** If you elect to make a Protected Disclosure with partial anonymity, the Service Provider will sanitise your report, by removing your name and any contact details that may enable your identity to be disclosed.
- 7.2.4. **Step 4:** The Protected Disclosure will be passed on by the Service Provider to the Aspen Ethics Committee based in South Africa. Aspen will, via the Service Provider, acknowledge receipt of your Protected Disclosure and provide feedback within the timelines prescribed under applicable laws. You may also request feedback by phone, email or online via the website, by quoting the case reference number.
- 7.3. Irrespective of the Internal Reporting Outlet used, the alleged improper conduct will be investigated. The investigation team may comprise internal or external parties, or a combination of both, depending on the nature and complexity of the matter reported. Aspen reserves the right to not investigate any alleged improper conduct in respect of which there is insufficient information, or if Aspen reasonably believes that the report was not based on reasonable grounds.
- 7.4. Aspen reserves the right to request, via the relevant Reporting Outlet, further specific information or substantiation in respect of the alleged improper conduct, prior to commencing its investigation.

8. WHISTLEBLOWER ANONYMITY

A person making a protected disclosure may advise that they wish to remain anonymous, or place restrictions on who knows their identity. Aspen and the Service Provider will comply with such requests and Aspen will use its best endeavours to investigate an anonymous disclosure. There may, however, be limitations in investigating the matter where the whistleblower chooses to remain anonymous.

9. CONFIDENTIALITY

- 9.1. All Protected Disclosures, and the whistleblower's identity (where this is disclosed or becomes known), are treated confidentially and will only be shared with a limited group of people on a strict need-to-know basis. Information will only be disclosed outside this small group if we are required to do so by law or an important public interest is at stake, such as public safety.
- 9.2. Where we are required by law to inform the person who is the subject of a Protected Disclosure that a complaint has been filed against them, the whistleblower's identity will not be disclosed and such notification will be deferred until the investigation has run its course. This is to protect you, the whistleblower, as well as to protect the integrity of the whistleblowing process.
- 9.3. In some cases, however, confidentiality cannot be guaranteed as the very fact of the investigation may serve to reveal the source of the information, the statement of the person raising the concern may be needed as part of evidence against the

perpetrator, or legal proceedings at a later stage may require the individual to appear as a witness.

- 9.4. Disciplinary action will be taken against any employee who makes an unauthorised disclosure of the identity of a person who makes a Protected Disclosure under this Policy, or of information that will likely lead to the identification of such person.

10. WHISTLEBLOWER PROTECTION

- 10.1. The protection of whistleblowers is fundamental to the success of the Aspen whistleblower process. It is also a right afforded by law in many jurisdictions in which Aspen operates. No employee who makes a disclosure based on reasonable grounds, and in accordance with this Policy will, **as a consequence of making a Protected Disclosure**, suffer retaliation, including being:

- 10.1.1. subjected to any disciplinary action;
- 10.1.2. dismissed, suspended, demoted, harassed or intimidated;
- 10.1.3. transferred against his or her will;
- 10.1.4. refused transfer or promotion;
- 10.1.5. subjected to a term or condition of employment or retirement which is altered or kept altered to his or her detriment;
- 10.1.6. refused a reference or provided with an adverse reference;
- 10.1.7. denied appointment to any employment, profession or office;
- 10.1.8. threatened with any of the above; or
- 10.1.9. otherwise adversely affected in his or her employment, including employment opportunities and work security.

- 10.2. The equivalent protection, where relevant, is also extended to any external organisation represented by the whistleblower, such as a supplier.

- 10.3. The above protection is not afforded to an individual who has opted to blow the whistle on his or her own improper conduct.

- 10.4. Where a whistleblower reports false information, knowing it to be false, the above protection will not be available to them, and if they are an employee they will face disciplinary action up to and including dismissal.

- 10.5. Retaliation against a whistleblower is viewed by Aspen in a very serious light. Accordingly an employee who retaliates against a whistleblower in violation of this Policy will be subject to disciplinary action, up to and including dismissal.

- 10.6. If a whistleblower feels they have suffered retaliation as a result of making a Protected Disclosure, they should immediately report such to the chairperson of the Aspen Ethics Committee as follows: RVerster@aspenpharma.com.

11. PERSONAL INFORMATION

- 11.1. Aspen companies are responsible for personal information processed in accordance with this Policy.
- 11.2. Personal information is disclosed as set out in **paragraph 5** above and to the Aspen Group company that needs access to the information in order to investigate the alleged improper conduct and take appropriate action.
- 11.3. For detailed information on how Aspen uses and discloses personal information, the protections we apply, the legal bases for our use of the personal information and your data protection rights, please refer to **Annexure A**.

12. FAIR TREATMENT OF INDIVIDUALS MENTIONED IN PROTECTED DISCLOSURES

- 12.1. Where the allegation of improper conduct has not been substantiated, the fact the investigation has been carried out, the results of the investigation, and the identity of any person who is the subject of the Protected Disclosure will remain confidential, unless the subject requests otherwise.
- 12.2. Subject to applicable laws, and **paragraph 9.2**, an employee who is the subject of a Protected Disclosure has the right to:
- 12.2.1. be informed as to the substance of the allegations;
 - 12.2.2. be given a reasonable opportunity to put their case (either orally or in writing) to the Aspen Ethics Committee; and
 - 12.2.3. be informed of the findings in respect of the Protected Disclosure.

13. IMPROPER USE OF THIS POLICY

- 13.1. This Policy should not be used for settling personal disputes or reporting complaints relating to an employee's own personal work related circumstances, such as the way he/she has been treated at work. In such cases, the applicable Aspen **grievance procedure** should be followed.
- 13.2. Any person who knowingly or deliberately submits a malicious report may be subject to penalties under applicable laws. In addition, where the person is an employee of Aspen, disciplinary action may be taken, up to and including termination of the employment relationship.

14. **ACCESS TO THIS POLICY**

This Policy is published on the Corporate Governance section of the Group's website.

[END]

ANNEXURE A: PRIVACY NOTICE

Capitalised terms have the meaning ascribed to them in the Whistleblowing Policy to which this Annexure A is appended.

1. INTRODUCTION

- 1.1. Aspen receives reports regarding alleged improper conduct in terms of the Aspen Group Whistleblowing Policy.
- 1.2. The Policy makes provision for various Internal Reporting Outlets, including the Tip-Offs Anonymous service managed by the Service Provider.
- 1.3. Should an individual submit a Protected Disclosure via any of the Internal Reporting Outlets, Aspen will process personal data of that individual (where the person has elected to disclose their identity), and of anyone else who may be named in the Protected Disclosure.
- 1.4. The **data controller** of any personal data that may be processed in connection with the Policy is the relevant Aspen employing entity and or Aspen Pharmacare Holdings Limited.

2. WHAT DATA DOES ASPEN PROCESS?

- 2.1. If your Protected Disclosure is made anonymously, none of your personal data will be processed in connection with the investigation.
- 2.2. If you choose to disclose your identity through any of the Internal Reporting Outlets, the Aspen recipient, or the Service Provider (as the case may be) will collect your personal information which may include your name, surname, email address, contact number and, if you are an employee of Aspen, the name of your employer, your employee number, business unit and location. The content of your Protected Disclosure will also be processed in connection with your personal information, which may include details of the relevant incident or event you have witnessed or wish to report, and details of any personal opinion or expressions you wish to make in connection with the incident.
- 2.3. If a Protected Disclosure is made about your alleged conduct or involvement in alleged improper conduct, the Aspen recipient, or the Service Provider (as the case may be) will in general collect your name, surname, alias or nickname, gender, and (where applicable) employee number, title, company, division, and contact information. Information will also be collected about the allegation that is reported, including the nature of the allegation.
- 2.4. Notwithstanding the basis on which the Protected Disclosure is made, all personal data provided via any of the Internal Reporting Outlets will be managed confidentially. Where the Protected Disclosure is submitted via the Tip-Offs

Anonymous service, the Service Provider will not disclose the whistleblower's personal data to Aspen without his or her consent.

3. HOW DOES THE COMPANY COLLECT DATA?

Any personal data processed in accordance with this Policy, including the personal data of the whistleblower or the individual(s) referred to in the Protected Disclosure, will be reported to us, whether by the whistleblower, or by the Service Provider (subject to prior consent), depending on the Internal Reporting Outlet used. Furthermore, additional personal data may be generated and processed through the course of any investigation into the alleged improper conduct.

4. WHAT ARE THE PURPOSES FOR WHICH DATA IS PROCESSED AND WHAT IS OUR LEGAL BASIS FOR CARRYING OUT THE PROCESSING?

4.1. Where we process personal information in connection with a Protected Disclosure, the overarching purpose is to facilitate the raising of concerns about improper conduct, the investigation of those concerns, and (where the concerns are found to be valid) taking appropriate action to address them, and prevent similar concerns from arising in the future.

4.2. This involves processing personal information to:

4.2.1. receive, discuss and (where applicable) sanitise the Protected Disclosure;

4.2.2. request additional information to substantiate the Protected Disclosure;

4.2.3. collate information received in a Protected Disclosure and make that information available to designated persons for investigation;

4.2.4. investigate the alleged improper conduct; and

4.2.5. provide feedback to the whistleblower, and make recommendations to Aspen companies.

4.3. Data protection laws require a valid legal ground to process personal information. We process the information where necessary to:

4.3.1. comply with our legal or regulatory obligations (for example, laws relating to the combating of bribery, and other laws that require us to operate whistleblowing hotlines);

4.3.2. meet our legitimate interests; or

4.3.3. protect the vital interests of the relevant individual or of another natural person.

- 4.4. The legitimate interests referred to above include our interests in addressing conduct which is contrary to our Code of Conduct, acting ethically and responsibly as a business, complying with laws, and protecting the environment and the health and safety of our employees.

5. RETENTION OF PERSONAL DATA

- 5.1. Personal data is retained for as long as it is required to satisfy the purpose for which it was collected.
- 5.2. The Service Provider will retain personal data for as long as is appropriate to investigate the matter and, where relevant, to complete actions relating to the outcome of any investigation, in both cases in accordance with applicable law and to comply with legal, regulatory or internal policy requirements.
- 5.3. In general, reports are retained in a secure and limited-access database in order for Aspen to retain an ability to respond to future legal claims in respect of associated actions. Aspen endeavours to ensure that personal data is kept as current as possible and that irrelevant or excessive personal data is deleted or made anonymous as soon as reasonably practicable.
- 5.4. Please note that some personal data may need to be kept for longer periods. In particular, we may keep some specific types of personal data for different periods of time, as required by applicable law or in order to comply with legal and regulatory obligations and for other legitimate business reasons.

6. DISCLOSURES OF PERSONAL DATA

- 6.1. Personal data of the whistleblower, where they have consented to the disclosure of their identity, and of those referred to in the report, can be accessed by or may be disclosed on a need-to know basis to:
- 6.1.1. the Aspen Ethics Committee and Aspen investigations team;
 - 6.1.2. the Service Provider, who receives the information submitted as part of a report, and receives feedback from Aspen companies on the report;
 - 6.1.3. internal and external advisors, which may include forensic companies, who assist with the investigation;
 - 6.1.4. Aspen companies who have a need to access information in a report, for example, if the outcome of the investigation recommends action against an employee, the investigation report will be provided to the relevant employer at Aspen, including the line manager and relevant member of the HR team;
 - 6.1.5. third parties who provide services to Aspen and the Service Provider, such as IT systems providers or hosting providers; and

- 6.1.6. courts, public bodies, law enforcement agents and litigants where laws require us to make a disclosure, such as where a report is found to be false, unsubstantiated and made maliciously, and the accused person seeks that disclosure as part of an action for libel or defamation.
- 6.2. The Company expects any third parties to process any personal data disclosed to them in accordance with applicable law, including with respect to data confidentiality and security. In particular, our contract with the Service Provider requires it to protect personal data, including withholding whistleblowers' identities where an anonymous Protected Disclosure is made or in instances where the whistleblower has not provided consent to disclose personal data.
- 6.3. Where these third parties act as a "data processor" they carry out their tasks on our behalf and upon our instructions for the above mentioned purposes. In this case, your personal data will only be disclosed to these parties to the extent necessary to provide the required services.
- 6.4. In addition, we may share personal data with national authorities in order to comply with a legal obligation to which we are subject. This is, for example, the case in the framework of imminent or pending legal proceedings or a statutory audit.

7. INTERNATIONAL TRANSFER OF PERSONAL DATA

- 7.1. The members of the Aspen Ethics Committee to whom Protected Disclosures are notified are based in South Africa. As a result, personal data will be transferred out of the country in which the matter was reported, to South Africa.
- 7.2. Transfer of personal data intra-Group within Aspen is governed by the Aspen Intra-Group Data Transfer Agreement.

8. NOTICE OF CHANGES

The Company may change or update this Privacy Notice at any time, in accordance with applicable laws.